A New Discriminant Algebra Construction

Owen Biesel, Alberto Gioia

Received: December 10, 2015
Revised: April 6, 2016

Communicated by Alexander Merkurjev

Abstract. A discriminant algebra operation sends a commutative ring R and an R-algebra A of rank n to an R-algebra $\Delta_{A/R}$ of rank 2 with the same discriminant bilinear form. Constructions of discriminant algebra operations have been put forward by Rost, Deligne, and Loos. We present a simpler and more explicit construction that does not break down into cases based on the parity of n. We then prove properties of this construction, and compute some examples explicitly.

2010 Mathematics Subject Classification: Primary 13B02; Secondary 14B25, 11R11, 13B40, 13C10
Keywords and Phrases: discriminant algebra, discriminant form, algebra of finite rank, étale algebra, polynomial law

Contents

1. Introduction

An n-fold covering map of topological spaces $X \to S$ has an associated 2-fold "orientation" covering, which on fibers is described by the set of orderings of the n-element fiber of X, up to reorderings by even permutations. The algebraic analogue producing a rank-2 étale algebra from a rank-n one is called the *discriminant algebra*, and we briefly review its classical constructions below.
Let $f(x)$ in $\mathbb{Q}[x]$ be an irreducible polynomial of degree n. Suppose the Galois group of f is the symmetric group S_n, and let $x_1, \ldots, x_n$ be the roots of f in its splitting field N. The subfield of N consisting of elements invariant under even permutations of those roots is called the *discriminant field* of $L \coloneqq \mathbb{Q}[x]/(f(x))$. It is formed by adjoining a square root of the discriminant of L over K, hence the name.
Following [10, §18], we may extend this operation to general rank-n separable algebras A over a field K of arbitrary characteristic: such an algebra corresponds to an n-element π_K-set X, where π_K is the absolute Galois group of K, and the discriminant *algebra* of A is the rank-2 separable algebra $\Delta_{A/K}$ corresponding to the 2-element set of *orientations* of X, orderings of X up to re-orderings by even permutations. (If the characteristic of K is not 2, then the discriminant algebra of A may again be presented as $K[x]/(x^2 - d)$, where $d \in K$ is the discriminant of A with respect to some K-basis; see [10, Proposition 18.24].) The same π-set construction applies more generally whenever R is a connected ring and A is a rank-n projective separable R-algebra, since there is still a contravariant equivalence between projective separable R-algebras and finite sets equipped with an action by a suitable profinite group π_R. In [20], William Waterhouse drops the connectedness hypothesis by interpreting étale rank-n algebras as S_n-torsors, and the discriminant algebra mapping from S_n-torsors to S_2-torsors is merely the one coming from the sign homomorphism $\mathrm{S}_n \to \mathrm{S}_2$.
Our goal in this paper is to extend the discriminant algebra construction even further to the case of R a ring and A a rank-n projective R-algebra, with no separability hypothesis. (In this paper, all rings and algebras are commutative, associative, and unital, so an R-algebra structure on A is merely a homomorphism of commutative rings $R \to A$.) The main feature we wish to keep is that the discriminant algebra of A should have the same discriminant as that of A; this is easy to check in the original motivating case of a finite separable algebra A over K in characteristic other than 2: If A has discriminant d with respect to some K-basis, then the discriminant algebra for A over K is $\Delta \cong K[x]/(x^2 - d)$. Since 2 is a unit, we may as well write $\Delta \cong K[x]/(x^2 - d/4)$, which, with respect to the K-basis $\{1, x\}$, also has discriminant

$$\det \begin{pmatrix} \mathrm{Tr}_{\Delta/K}(1) & \mathrm{Tr}_{\Delta/K}(x) \\ \mathrm{Tr}_{\Delta/K}(x) & \mathrm{Tr}_{\Delta/K}(x^2) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & d/2 \end{pmatrix} = d.$$

In this paper, we put forth such a general discriminant algebra construction. In the setting of a ring R and algebra A that is locally free of rank n as an R-module, it still makes sense to talk about the trace and discriminant maps:

A has a *discriminant bilinear form* $\delta_{A/R}$ on $\bigwedge^n A$ defined by

$$\delta_{A/R}(a_1 \wedge \cdots \wedge a_n, b_1 \wedge \cdots \wedge b_n) = \det\big(\mathrm{Tr}_{A/R}(a_i b_j)\big)_{ij}.$$

Here is the first main result of this paper:

Theorem 1 (proven as Theorem 4.1). *There is an assignment $(R, A) \mapsto \Delta_{A/R}$ sending any rank-n algebra A over any ring R to a rank-2 R-algebra $\Delta_{A/R}$ that is endowed with a canonical isomorphism $\bigwedge^2 \Delta_{A/R} \cong \bigwedge^n A$ identifying the discriminant bilinear form of $\Delta_{A/R}$ with that of A.*

We call $\Delta_{A/R}$ the *discriminant algebra* of A over R. In a 2005 letter to Manjul Bhargava and Markus Rost, Pierre Deligne suggested a list of four other properties a discriminant algebra operation $(R, A) \mapsto \Delta_{A/R}$ should have; see [5] for the original formulation. We prove that these properties hold for our construction with the following theorems; the first property is that forming the discriminant algebra should commute with base change:

Theorem 2 (proven as Theorem 6.1). *If R is a ring and A is an R-algebra of rank n, and R' is any R-algebra, let A' denote $R' \otimes_R A$, an R'-algebra of rank n. Then there is a canonical isomorphism $R' \otimes_R \Delta_{A/R} \cong \Delta_{A'/R'}$.*

Deligne's second requirement is an explicit description of the discriminant algebra in the case that 2 is invertible, and is a generalization of the idea of adjoining to the base ring a square root of the discriminant of the algebra with respect to some basis.

Theorem 3. *If 2 is a unit in R and A is an R-algebra of rank n, then there is an R-algebra isomorphism $\Delta_{A/R} \xrightarrow{\sim} R \oplus \bigwedge^n A$, where the latter is given the R-algebra structure whose identity element is $(1, 0)$, and where the product of two elements $a, b \in \bigwedge^n A$ is via the discriminant form: $a \cdot b \coloneqq \delta_{A/R}(a, b) \in R$.*

We will find that it actually makes more sense to include a factor of $1/4$ in the multiplication, so that the product of two elements $a, b \in \bigwedge^n A$ is $\frac{1}{4}\delta_{A/R}(a, b)$. (This is analogous to presenting the discriminant algebra of a separable K-algebra with discriminant d as $K[x]/(x^2 - d/4)$ instead of $K[x]/(x^2 - d)$.) Then Theorem 3 is actually a consequence of Theorem 1; see Corollary 6.3.
Deligne's third requirement is that in the case of R connected and A étale over R, the discriminant algebra for A over R should be the one described at the beginning of the introduction:

Theorem 4 (proven as Theorem 6.8). *Let R be a connected ring and A an étale R-algebra of rank n corresponding to a π_R-set X. Then $\Delta_{A/R}$ is also étale, and corresponds to the 2-element set $\mathrm{Or}(X)$ of orientations of X.*

Deligne's fourth requirement was that the two descriptions of $\Delta_{A/R}$ from Theorems 3 and 4 should be compatible when both apply, and we omit the statement here. In his letter, Deligne sketched a construction of an operation $(R, A) \mapsto \Delta^{\mathrm{Del}}_{A/R}$ satisfying his four properties. He first reduced to a similar list of properties that a discriminant algebra operation for quadratic forms should have, and extended the corresponding étale and 2-invertible descriptions across their codimension-2 complement in a universal case. This construction only works for odd-rank algebras, so he defined the discriminant algebra of an even-rank A to be that of $R \times A$. However, he does not specifically equip $\Delta^{\mathrm{Del}}_{A/R}$ with the structure of a discriminant-identifying isomorphism $\bigwedge^2 \Delta^{\mathrm{Del}}_{A/R} \cong \bigwedge^n A$. Earlier, Markus Rost had exhibited in [16] a way of producing a natural rank-2 algebra $K_{A/R}$ from a rank-3 R-algebra A, but it admits no natural discriminant-identifying isomorphism $\bigwedge^2 K_{A/R} \cong \bigwedge^3 A$. Rost fixed this defect by the process of Verschiebung or "shifting": modifying the multiplication of $K_{A/R}$ to obtain a new quadratic algebra $\Delta^{\mathrm{Rost}}_{A/R}$ with the desired discriminant form. Ottmar Loos later employed this shifting technique to give a discriminant algebra construction in [13] for even-rank algebras, extending to the odd-rank case again by defining $\Delta^{\mathrm{Loos}}_{A/R} \coloneqq \Delta^{\mathrm{Loos}}_{(R\times A)/R}$ when A has odd rank.

The main advantages of our discriminant algebra construction $(R, A) \mapsto \Delta_{A/R}$ are that it does not appeal to a separate construction for quadratic forms, it does not split into cases based on whether the rank of A is odd or even, and it does not require first handling special cases (such as 2 being invertible or the algebra being étale).

Namely, given a ring R and an R-algebra A of rank n, there is a canonical R-algebra homomorphism from the S_n-invariant tensors of $A^{\otimes n}$ to R; we call this the *Ferrand homomorphism* $\Phi_{A/R}\colon (A^{\otimes n})^{\mathrm{S}_n} \to R$. Then we use the Ferrand homomorphism to define the discriminant algebra of A over R as the tensor product

$$\Delta_{A/R} \coloneqq (A^{\otimes n})^{\mathrm{A}_n} \bigotimes_{(A^{\otimes n})^{\mathrm{S}_n}} R.$$

In Section 2, we define the Ferrand homomorphism and discriminant algebra associated to a rank-n algebra. We prove Theorem 1 in Section 4, and prove Theorems 2 to 4 in Section 6. In between, in Section 3 we discuss the action of the Ferrand homomorphism, and Section 5 exhibits some examples of discriminant algebras. Section 7 shows that the construction of the discriminant algebra is functorial with respect to algebra homomorphisms that preserve the characteristic polynomial of every element.

In Section 8, we analyze the discriminant algebra of a product algebra; our main result is that $\Delta_{(A\times B)/R} \cong \Delta_{A/R} * \Delta_{B/R}$, where $*$ is the commutative monoid structure on the set of isomorphism classes of quadratic algebras, characterized by John Voight in [19]. We also show that $\Delta_{(R\times A)/R} \cong \Delta_{A/R}$, so that if we set $\Delta_{A/R} \coloneqq R^2$ for A of rank 0 or 1, we obtain a monoid homomorphism from the set of isomorphism classes of (locally) constant-rank algebras to the set of isomorphism classes of quadratic algebras, carrying $\times$ to $*$.

In forthcoming work, the authors exhibit isomorphisms between this discriminant algebra construction and those given by Rost and Loos. The isomorphism with Loos's discriminant algebra is quite subtle, and suggests that there may be only one discriminant algebra operation satisfying Theorems 1 to 4 up to isomorphism. Due to the existence of suitably nice universal cases, the authors have been able to verify this uniqueness in ranks up to 3, but the general case is still unknown.

Both authors would like to thank Lenny Taelman for several helpful discussions throughout this project, as well as Darij Grinberg and the anonymous referee for their comments and corrections. The second author would also like to thank the Austrian Science Fund FWF for its support through project P25652.

2. Defining the Ferrand homomorphism and discriminant algebra

Given a ring R with algebra A of rank n, Daniel Ferrand in [6] uses a certain homomorphism $\Phi_{A/R}\colon (A^{\otimes n})^{\mathrm{S}_n} \to R$ to construct a functor from A-modules to R-modules. We call this homomorphism the *Ferrand homomorphism*.

In case K is a field and L is a degree-n separable field extension of K, then the Ferrand homomorphism $\Phi_{L/K}$ has a simple description, given the Galois closure N of L over K: Compile the n homomorphisms $L \to N$ over K into a single homomorphism $L^{\otimes n} \to N$, and restrict it to the subalgebra $(L^{\otimes n})^{\mathrm{S}_n}$. The image in N of any S_n-invariant tensor will be invariant under the Galois action on N, and thus belongs to K, giving us the Ferrand homomorphism $\Phi_{L/K}\colon (L^{\otimes n})^{\mathrm{S}_n} \to K$.

In this section, we will briefly review Ferrand's abstract definition of the Ferrand homomorphism in [6], and then we will describe how to compute its action on symmetric tensors.

First, we recall the setting in which elements of algebras have norms. Thus an algebra over a ring R is just another ring A with a ring homomorphism $R \to A$.

Definition 2.1. Let R be a ring, and let M be an R-module. We say that M is *locally free (of rank n)* if there are elements $r_1, \dots, r_k \in R$, together generating the unit ideal, such that M_{r_i} is free (of rank n) as an R_{r_i}-module for each $i \in \{1, \dots, k\}$. An R-algebra A is said to be *of rank n* if A is locally free of rank n as an R-module.

Remark 2.2. Equivalently, an R-module M is locally free of rank n if and only if it is projective and finitely generated (i.e. flat and finitely presented) and the rank of each (necessarily free) $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ is n for each prime ideal $\mathfrak{p} \in M$; see [3, Thm. 2 on p. II.141].

The following observation about locally free algebras and modules will be useful throughout this paper:

Lemma 2.3. *Let R be a ring and A an R-algebra of rank $n \geq 2$. Then the quotient A/R is a locally-free R-module of rank $n-1$, and the natural map*

$$\bigwedge^{n-1}(A/R) \to \bigwedge^n A$$

sending $[a_1] \wedge \cdots \wedge [a_{n-1}]$ to $1 \wedge a_1 \wedge \cdots \wedge a_{n-1}$ is an isomorphism.

In particular, if A is a quadratic (i.e. rank-2) R-algebra then there is a canonical isomorphism $A/R \to \bigwedge^2 A$ sending the class of a to $1 \wedge a$.

Proof. For the first claim, that A/R is locally free, it is enough to show that A/R is flat and finitely presented. First, the structure morphism $R \to A$ is injective since the rank of A is everywhere positive, and since the same applies after base change to any R-algebra, we find that $R \to A$ is the inclusion of a pure submodule. The quotient of a flat module by a pure submodule is also flat, so the quotient A/R is a flat R-module. It is also finitely presented, since A is, so A/R is locally free.
The claims that A/R has rank $n-1$ and that the given map on exterior powers is an isomorphism can be checked locally, so assume R is a local ring. Then A/R is a free R-module, so let $\{[\theta_1], \dots, [\theta_k]\}$ be an R-basis for it. Then A is has R-basis $\{1, \theta_1, \dots, \theta_k\}$, so since A has rank n we must have $k = n-1$ as desired. Finally, note that the indicated homomorphism $\bigwedge^{n-1}(A/R) \to \bigwedge^n A$ maps the singleton basis $\{[\theta_1] \wedge \cdots \wedge [\theta_{n-1}]\}$ to the basis $\{1 \wedge \theta_1 \wedge \cdots \wedge \theta_{n-1}\}$, so is an isomorphism. $\square$

Definition 2.4. Let R be a ring, and let A be an R-algebra of rank n. For each element $a \in A$, multiplication by a is an R-module homomorphism $A \to A$, and the nth exterior power of this homomorphism is an R-module homomorphism $\bigwedge^n A \to \bigwedge^n A$. Since $\bigwedge^n A$ is locally free of rank 1, this endomorphism is equal to multiplication by a unique element of R, called the *norm* $\mathrm{Nm}_{A/R}(a)$ of a.

What sort of map is $\mathrm{Nm}_{A/R}\colon A \to R$? It is multiplicative, but almost never additive, and thus it is not a ring homomorphism. It is, however, the base component of a *multiplicative homogeneous degree-n polynomial law*:

Definition 2.5. Let R be a ring and M and N two R-modules. A *polynomial law* $p\colon M \to N$ is a collection of functions $p_S\colon S \otimes_R M \to S \otimes_R N$ for each R-algebra S, such that for every R-algebra homomorphism $f\colon S \to S'$ the following square of functions commutes:

$$\begin{tikzcd} S \otimes_R M \arrow[r, "p_S"] \arrow[d, "f\otimes \mathrm{id}_M"'] & S \otimes_R N \arrow[d, "f\otimes \mathrm{id}_N"] \\ S' \otimes_R M \arrow[r, "p_{S'}"] & S' \otimes_R N \end{tikzcd}$$

We say that p is *homogeneous of degree n* if for every R-algebra S, element $s \in S$ and element $m \in S \otimes M$, we have $p_S(sm) = s^n p_S(m)$. If $p\colon A \to B$ is a polynomial law between two R-algebras A and B, we say p is *multiplicative* if each $p_S\colon S \otimes_R A \to S \otimes_R B$ is a multiplicative function.

For example, if A is an R-algebra, then the diagonal function $A \to A^{\otimes n}$ sending a to $a \otimes \cdots \otimes a$ extends naturally to a multiplicative homogeneous degree-n polynomial law $A \to A^{\otimes n}$.
A fundamental result of the theory of polynomial laws, developed by Norbert Roby in [14], is that for each R-module M there is a universal homogeneous degree-n polynomial law $\gamma^n\colon M \to \Gamma^n_R(M)$; every homogeneous degree-n polynomial law $M \to N$ factors uniquely as γ^n followed by an ordinary R-module

homomorphism $\Gamma^n_R(M) \to N$. Furthermore, Roby shows in [15] that if A is an R-algebra, then $\Gamma^n_R(A)$ is also an R-algebra and *multiplicative* degree-n polynomial laws $A \to B$ correspond to R-*algebra* homomorphisms $\Gamma^n_R(A) \to B$. Thus the norm map $\mathrm{Nm}_{A/R} \colon A \to R$ corresponds to an R-algebra homomorphism $\Gamma^n_R(A) \to R$.

A general presentation for $\Gamma_R(M)$ may be found in [14, III.1], but for our purposes it is sufficient to note that the diagonal polynomial law $A \to A^{\otimes n}$ gives us an R-algebra homomorphism $\Gamma^n_R(A) \to A^{\otimes n}$, and that if A is a flat R-algebra then this homomorphism restricts to an isomorphism with the subalgebra of S_n-invariant tensors (see [4, 5.5.2.5 on p. 123]):

$$\Gamma^n_R(A) \xrightarrow{\sim} (A^{\otimes n})^{\mathrm{S}_n} : \gamma^n(a) \mapsto a \otimes \cdots \otimes a.$$

Thus if A and B are R-algebras with A flat, multiplicative homogeneous degree-n polynomial laws $A \to B$ correspond to R-algebra homomorphisms $(A^{\otimes n})^{\mathrm{S}_n} \to B$.

Definition 2.6 (c.f. [6, 3.1.2]). Let R be a ring and A an R-algebra of rank n. Then the norm polynomial law $\mathrm{Nm}_{A/R} \colon A \to R$ corresponds to an R-algebra homomorphism

$$\Phi_{A/R} \colon (A^{\otimes n})^{\mathrm{S}_n} \cong \Gamma^n_R(A) \to R,$$

called *the Ferrand homomorphism* (of A over R). It is the unique R-algebra homomorphism such that for every R-algebra R' and every element $a \in A' \coloneqq R' \otimes_R A$, the composite

$$(A'^{\otimes_{R'} n})^{\mathrm{S}_n} \xrightarrow{\sim} R' \otimes_R (A^{\otimes n})^{\mathrm{S}_n} \xrightarrow{\mathrm{id}_{R'} \otimes \Phi_{A/R}} R' \otimes_R R \xrightarrow{\sim} R' \tag{1}$$

sends $a \otimes \cdots \otimes a$ to $\mathrm{Nm}_{A'/R'}(a) \in R'$.

As an immediate corollary to this definition, we find for each R-algebra R' and $A' \coloneqq R' \otimes_R A$ that the composite (1) is the Ferrand homomorphism for A' over R'. We say that the Ferrand homomorphism *commutes with base change.*

Definition 2.7. Let R be a ring and let A be an R-algebra of rank n with $n \geq 2$. Then the *discriminant algebra* $\Delta_{A/R}$ *of* A *over* R is the tensor product of $(A^{\otimes n})^{\mathrm{S}_n}$-algebras

$$\Delta_{A/R} = (A^{\otimes n})^{\mathrm{A}_n} \bigotimes_{(A^{\otimes n})^{\mathrm{S}_n}} R$$

defined by the inclusion $(A^{\otimes n})^{\mathrm{S}_n} \hookrightarrow (A^{\otimes n})^{\mathrm{A}_n}$ and the Ferrand homomorphism $\Phi_{A/R} \colon (A^{\otimes n})^{\mathrm{S}_n} \to R$.

If the base ring R is understood, it may be omitted and the discriminant algebra of A denoted Δ_A. We will adopt similar conventions for the trace and norm maps, the Ferrand homomorphism, and the discriminant bilinear form.

Remark 2.8. Note that since the Ferrand homomorphism $\Phi_{A/R}$ is surjective, so is the homomorphism from $(A^{\otimes n})^{\mathrm{A}_n} \to \Delta_{A/R}$. Thus $\Delta_{A/R}$ can be understood as the quotient of $(A^{\otimes n})^{\mathrm{A}_n}$ by the ideal generated by elements of the form $x - \Phi_{A/R}(x)$ for $x \in (A^{\otimes n})^{\mathrm{S}_n}$. If x is a general element of $(A^{\otimes n})^{\mathrm{A}_n}$, we will often denote its image in $\Delta_{A/R}$ by $\dot{x}$.

Remark 2.9. Note that if we replace $(A^{\otimes n})^{\mathrm{A}_n}$ by $A^{\otimes n}$ in the definition of $\Delta_{A/R}$, we obtain what Ferrand denotes by $\mathbf{P}^{(1,\dots,1)}(A)$ in [6, 5.2] and what Bhargava calls the S_n*-closure of* A *over* R in [1].
Denoting the S_n-closure by B, we thus obtain an R-algebra homomorphism $\Delta_{A/R} \to B$ by tensoring the inclusion $(A^{\otimes n})^{\mathrm{A}_n} \hookrightarrow A^{\otimes n}$ along $\Phi_{A/R}$. In case $R \to A$ is a degree-n separable field extension $K \hookrightarrow L$ in characteristic other than 2, whose normal closure N has Galois group S_n, then $B \cong N$ and this homomorphism $\Delta_{A/R} \to B$ is just the inclusion of the discriminant field of L into N.

3. Understanding the Ferrand homomorphism

The two defining facts of the Ferrand homomorphisms are that they send elements of the form $a \otimes \cdots \otimes a$ to the norm of a, and that they commute with base change. Our primary tool for computing the image of an arbitrary symmetric tensor, then, is to identify it as a term in some tensor power of a single element, and then correspondingly break up the norm of that single element.
For example, if A is any R-algebra, and $a \in A$, then we have the following elements of $(A^{\otimes n})^{\mathrm{S}_n}$:

$$\begin{aligned}
e_1(a) &\coloneqq (a \otimes 1 \otimes \cdots \otimes 1) + (1 \otimes a \otimes \cdots \otimes 1) + \ldots + (1 \otimes \cdots \otimes 1 \otimes a)\\
e_2(a) &\coloneqq (a \otimes a \otimes 1 \otimes \cdots \otimes 1) + (a \otimes 1 \otimes a \otimes \cdots \otimes 1) + \ldots\\
&\qquad \ldots + (1 \otimes \cdots \otimes 1 \otimes a \otimes a)\\
&\cdots\\
e_n(a) &\coloneqq (a \otimes a \otimes \cdots \otimes a).
\end{aligned}$$

These are the elementary symmetric polynomials in the n elements $a^{(1)}, \dots, a^{(n)} \in A^{\otimes n}$, where $a^{(i)}$ is the element

$$a^{(i)} = 1 \otimes \cdots \otimes 1 \otimes a \otimes 1 \otimes \cdots \otimes 1 \tag{2}$$

with the a in the ith tensor factor.
In case A is a rank-n R-algebra, we can compute the image of $e_k(a)$ under $\Phi_{A/R} \colon (A^{\otimes n})^{\mathrm{S}_n} \to R$ as follows: First, note that $e_k(a)$ is the coefficient of $\lambda^{n-k}\mu^k$ in $(\lambda+\mu a) \otimes \cdots \otimes (\lambda + \mu a)$, as an element of $(A[\lambda,\mu]^{\otimes_{R[\lambda,\mu]} n})^{\mathrm{S}_n}$. (Thus we sometimes also write $e_0(a) = 1$.) The image of this element under $\Phi_{A[\lambda,\mu]/R[\lambda,\mu]}$ is its norm $f(\lambda,\mu) \in R[\lambda,\mu]$. Since the norm map is homogeneous of degree n, we find that $f(\lambda,\mu)$ is a homogeneous polynomial of degree n; denoting by $s_k(a)$ the coefficient of $\lambda^{n-k}\mu^k$ in $f(\lambda,\mu)$, we obtain

$$\Phi_{A[\lambda,\mu]/R[\lambda,\mu]} \colon \sum_{k=0}^{n} e_k(a)\lambda^{n-k}\mu^k \mapsto \sum_{k=0}^{n} s_k(a)\lambda^{n-k}\mu^k.$$

Since $\Phi_{A[\lambda,\mu]/R[\lambda,\mu]}$ is just $\Phi_{A/R} \otimes \mathrm{id}_{R[\lambda,\mu]}$, we thus have

$$\Phi_{A/R} \colon e_k(a) \mapsto s_k(a)$$

for each $k \in \{0, \dots, n\}$.
What are these quantities $s_k(a) \in R$? The answer comes by setting $\mu = -1$, so that

$$\sum_{k=0}^{n} s_k(a)\lambda^{n-k}(-1)^k = \mathrm{Nm}_{A[\lambda]/R[\lambda]}(\lambda - a),$$

the characteristic polynomial of a. We can thus read off $s_k(a)$ as $(-1)^k$ times the coefficient of λ^{n-k} in the characteristic polynomial of a. In particular, $s_n(a)$ is the norm $\mathrm{Nm}_{A/R}(a)$ of a, and $s_1(a)$ is its trace $\mathrm{Tr}_{A/R}(a)$.
We summarize the above discussion in the following lemma:

LEMMA 3.1. *Let R be a ring and A an R-algebra with an element $a \in A$, and let $k \in \{0, \dots, n\}$. Denote by $e_k(a)$ the kth elementary symmetric polynomial in the n elements $a^{(1)}, \dots, a^{(n)} \in A^{\otimes n}$ defined in* (2)*. Now suppose A is a rank-n R-algebra, and let $s_k(a)$ be $(-1)^k$ times the coefficient of λ^{n-k} in the characteristic polynomial of a. Then $\Phi_{A/R}\big(e_k(a)\big) = s_k(a)$.*

We can similarly compute the image under $\Phi_{A/R}$ of other elements of $(A^{\otimes n})^{\mathrm{S}_n}$.

DEFINITION 3.2 (c.f. [6, 2.2.3.1]). Let $a = (a_i)_{i\in I} \in A^I$ be a tuple of elements of A, and let $\alpha \subseteq I^n$. We define an element $\gamma^\alpha(a) \in A^{\otimes n}$ by

$$\gamma^\alpha(a) \coloneqq \sum_{(i_1,\dots,i_n)\in\alpha} a_{i_1} \otimes \cdots \otimes a_{i_n}.$$

If G is a subgroup of S_n and α is invariant under the action of G on I^n, then $\gamma^\alpha(a) \in (A^{\otimes n})^G$. For example, if α is the S_n-orbit of $(i_1, \dots, i_n) \in I^n$, then $\gamma^\alpha(a)$ is the coefficient of $\lambda_{i_1} \dots \lambda_{i_n}$ in $(\sum_{i\in I} \lambda_i a_i) \otimes \cdots \otimes (\sum_{i\in I} \lambda_i a_i)$. In this case $\Phi_{A/R}(\gamma^\alpha(a))$ is the coefficient of $\lambda_1 \dots \lambda_n$ in the norm of $\sum_{i\in I} \lambda_i a_i$, as an element of the rank-n $R[\lambda_i : i \in I]$-algebra $A[\lambda_i : i \in I]$. The case of $\Phi_{A/R}(e_k(a)) = s_k(a)$ is recovered by taking $I = \{1, 2\}$ and $(a_1, a_2) = (1, a)$.
In general, we will write the set of G-orbits of I^n as I^n/G, and write $\alpha \in I^n/G$ to mean that α is one such G-orbit.

We will often consider the case that the tuple $I \to A$ is an ordinary n-tuple $a = (a_1, \dots, a_n) \in A^n$, and that the subset $\alpha \subseteq \{1, \dots, n\}^n = \mathrm{Map}(\{1, \dots, n\}, \{1, \dots, n\})$ is a subgroup $G \subseteq \mathrm{S}_n$, or a coset σG of G. (The most common cases are $G = \mathrm{S}_n$ or A_n, or the coset of odd permutations $\overline{\mathrm{A}}_n$.) The quantity $\gamma^{\sigma G}(a_1, \dots, a_n)$ is linear in each a_i, since each a_i appears exactly once per term as one of the tensor factors.

EXAMPLE 3.3. Consider the case $R = \mathbb{Z}$ and $A = R[x]/(x^2+x+2)$, a quadratic R-algebra. If we set $a_1 = -2x + 1$ and $a_2 = 3x + 2$, then the element $a_1 \otimes a_2 + a_2 \otimes a_1$ is an S_2-invariant element of $A^{\otimes 2}$—what is its image under the Ferrand homomorphism $\Phi_{A/R}\colon (A^{\otimes 2})^{\mathrm{S}_2} \to R$? We will calculate the answer three different ways to demonstrate the various methods we will use throughout the paper.
First, and simplest, note that since $x \in A$ satisfies both the defining equation $x^2+x+2 = 0$ as well as its characteristic polynomial $x^2 - \mathrm{Tr}_A(x) + \mathrm{Nm}_A(x) = 0$,

we find that these two equations are equal because 1 and x are R-linearly independent elements of A. Therefore $\mathrm{Tr}_A(x) = -1$ and $\mathrm{Nm}_A(x) = 2$. We can then compute the image of $a_1 \otimes a_2 + a_2 \otimes a_1$ by expanding it in terms of these quantities:

$$\begin{aligned}
a_1 \otimes a_2 + a_2 \otimes a_1 &= (-2x+1) \otimes (3x+2) + (3x+2) \otimes (-2x+1) \\
&= -6(x \otimes x) - 4(x \otimes 1) + 3(1 \otimes x) + 2(1 \otimes 1) \\
&\quad - 6(x \otimes x) + 3(x \otimes 1) - 4(1 \otimes x) + 2(1 \otimes 1) \\
&= -12(x \otimes x) - 1(x \otimes 1 + 1 \otimes x) + 4 \\
&= -12 \cdot e_2(x) - 1 \cdot e_1(x) + 4 \\
&\mapsto -12 \cdot s_2(x) - 1 \cdot s_1(x) + 4 \\
&= -12 \cdot \mathrm{Nm}_A(x) - 1 \cdot \mathrm{Tr}_A(x) + 4 \\
&= -12 \cdot 2 - 1 \cdot -1 + 4 = -19.
\end{aligned}$$

We can also determine the image of $a_1 \otimes a_2 + a_2 \otimes a_1$ knowing only how multiplying by a_1 and a_2 act with respect to an R-basis of A. Choosing the R-basis $\{1, x\}$, we find that they act by the matrices

$$a_1 : \begin{pmatrix} 1 & 4 \\ -2 & 3 \end{pmatrix} \qquad a_2 : \begin{pmatrix} 2 & -6 \\ 3 & -1 \end{pmatrix}.$$

(For example, $a_2 \cdot x = (3x+2)(x) = 3x^2 + 2x = 3(-x-2) + 2x = -6 - x$, whose coefficients are found in the second column of the a_2 matrix.) Now $a_1 \otimes a_2 + a_2 \otimes a_1$ is the quantity denoted $\gamma^{\mathrm{S}_2}(a_1, a_2)$, which is the coefficient of $\lambda_1\lambda_2$ in $(\lambda_1 a_1 + \lambda_2 a_2) \otimes (\lambda_1 a_1 + \lambda_2 a_2)$. Thus its image under the Ferrand homomorphism is the coefficient of $\lambda_1\lambda_2$ in the norm of $\lambda_1 a_1 + \lambda_2 a_2$ (as an element of the quadratic $R[\lambda_1, \lambda_2]$-algebra $A[\lambda_1, \lambda_2]$). This element acts by the matrix

$$\lambda_1 a_1 + \lambda_2 a_2 : \begin{pmatrix} \lambda_1 + 2\lambda_2 & 4\lambda_1 - 6\lambda_2 \\ -2\lambda_1 + 3\lambda_2 & 3\lambda_1 - \lambda_2 \end{pmatrix}.$$

Ignoring all but the $\lambda_1\lambda_2$ terms, this determinant is

$$(\lambda_1)(-\lambda_2) + (2\lambda_2)(3\lambda_1) - (4\lambda_1)(3\lambda_2) - (-6\lambda_2)(-2\lambda_1) = -19\lambda_1\lambda_2,$$

so $\Phi_{A/R}(a_1 \otimes a_2 + a_2 \otimes a_1) = -19$, as before.

Finally, note that we can write $a_1 \otimes a_2 + a_2 \otimes a_1$ as a polynomial in symmetric tensors of the form $e_k(f)$:

$$\begin{aligned}
a_1 \otimes a_2 + a_2 \otimes a_1 &= (a_1 \otimes 1 + 1 \otimes a_1)(1 \otimes a_2 + a_2 \otimes 1) \\
&\quad - (a_1 a_2 \otimes 1 + 1 \otimes a_1 a_2) \\
&= e_1(a_1) e_1(a_2) - e_1(a_1 a_2) \\
&\mapsto s_1(a_1) s_1(a_2) - s_1(a_1 a_2) \\
&= \mathrm{Tr}_A(a_1)\mathrm{Tr}_A(a_2) - \mathrm{Tr}_A(a_1 a_2).
\end{aligned}$$

We can read off $\mathrm{Tr}_A(a_1)$ and $\mathrm{Tr}_B(a_2)$ as the traces of the above matrices, namely $1 + 3 = 4$ and $2 - 1 = 1$. The trace of $a_1 a_2$ can by computed similarly as the trace of the product matrix:

$$a_1a_2 : \begin{pmatrix} 1 & 4 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 2 & -6 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} 14 & -10 \\ 5 & 9 \end{pmatrix},$$

so $\mathrm{Tr}_A(a_1a_2) = 14+9 = 23$. Therefore $\Phi_A(a_1 \otimes a_2 + a_2 \otimes a_1) = (4)(1) - (23) = -19$.

The latter two methods for computing $\Phi_{A/R}$ of an S_n-invariant tensor—expanding the tensor as a linear combination of the $\gamma^\alpha(a)$ or a polynomial in the $e_k(a)$—will be used throughout this paper. The remainder of this section consists of technically useful results on sets of module and algebra generators for the G-invariants of tensor powers, which, in effect, say that the methods of Example 3.3 will always be sufficient to calculate the image of an S_n-invariant tensor under the Ferrand homomorphism.

Lemma 3.4. *Let R be a ring and M a projective R-module. Let $\theta = (\theta_i)_{i\in I} \in M^I$ be a generating family (resp. R-basis) for M. Then for each natural number d and subgroup $G \subseteq \mathrm{S}_d$, the family $\{\gamma^\alpha(\theta) : \alpha \in I^d/G\}$ is a generating family (resp. R-basis) for $(M^{\otimes d})^G$.*

Recall that by $\alpha \in I^d/G$ we mean that α is an orbit of I^d under the action of G, so that the notation $\gamma^\alpha(\theta)$ makes sense.

Proof. First consider the case in which θ is an R-basis for M. Then every tensor in $M^{\otimes d}$ can be uniquely represented as an R-linear combination of pure tensors of the form $\theta_{i_1} \otimes \cdots \otimes \theta_{i_d}$. Such a linear combination is G-invariant precisely if the coefficients are constant across G-orbits of the pure tensors, i.e. if the tensor is an R-linear combination of the $\gamma^\alpha(\theta)$ as α ranges over I^d/G. Hence the $\gamma^\alpha(\theta)$ generate $(M^{\otimes d})^G$. Furthermore, since no pure tensor is a term in more than one of the $\gamma^\alpha(\theta)$, they are also R-linearly independent, and hence form an R-basis for $(M^{\otimes d})^G$.

Second, suppose that M is merely projective and that $\{\theta_i : i \in I\}$ merely generates M as an R-module. Then let $R^{(I)}$ be the free R-module with basis $e = (e_i)_{i\in I}$, and $R^{(I)} \twoheadrightarrow M$ be the surjection sending e_i to θ_i. Since M is projective, this surjection has a right inverse, which is a property preserved by any functor. Hence after applying the functor $((\cdot)^{\otimes d})^G$, we obtain another surjection $((R^{(I)})^{\otimes d})^G \twoheadrightarrow (M^{\otimes d})^G$. Since $\{\gamma^\alpha(e) : \alpha \in I^d/G\}$ generates $((R^{(I)})^{\otimes d})^G$ by the above, its image $\{\gamma^\alpha(\theta) : \alpha \in I^d/G\}$ generates $(M^{\otimes d})^G$ as well. $\square$

Thus given a set of R-module generators $\theta = (\theta_i)_{i\in I}$ of a rank-n R-algebra A, we find that every element of $(A^{\otimes n})^{\mathrm{S}_n}$ (resp. $(A^{\otimes n})^{\mathrm{A}_n}$) can be written as an R-linear combination of the $\gamma^\alpha(\theta)$, as α ranges over all S_n-orbits (resp. A_n-orbits) of I^n. This fact has a number of consequences that we explore in the remainder of this section.

Proposition 3.5. *Let R be a ring, let M be a locally free R-module, let d be a natural number, and let G be a subgroup of S_d. Let R' be any R-algebra, and* *denote by M' the locally free R'-module $R' \otimes_R M$. Then the natural R'-module homomorphism $R' \otimes_R (M^{\otimes d})^G \to (M'^{\otimes_{R'} d})^G$ is an isomorphism.*

Proof. Since $(M^{\otimes d})^G$ can be written as an equalizer of finitely many maps $M^{\otimes d} \to M^{\otimes d}$, the functor $((\cdot)^{\otimes d})^G$ commutes with localization (see, for example, [9, Prop. A7.1.3]). We therefore only need to check that the given homomorphism is an isomorphism in the case that M is free. Say M has R-basis $\theta = (\theta_i)_{i \in I}$, so that M' has a free R'-basis $\theta' = (1 \otimes \theta_i)_{i \in I}$. Then the canonical map $R' \otimes_R (M^{\otimes d})^G \to (M'^{\otimes_{R'} d})^G$ carries the R'-basis $\{1 \otimes \gamma^\alpha(\theta) : \alpha \in I^d/G\}$ to the R'-basis $\{\gamma^\alpha(\theta') : \alpha \in I^d/G\}$, so is an isomorphism. $\square$

Next we show that elements of the form $e_k(a)$ generate $(A^{\otimes n})^{\mathrm{S}_n}$ as an algebra. The proof is algorithmic in nature, and shows us how to write any element of the form $\gamma^\alpha(a)$ as a polynomial in the $e_k(a)$.

Lemma 3.6. *Let R be a ring and A a rank-n R-algebra. Let $\Omega \subseteq A$ be a set of elements of A whose powers together generate A as an R-module. Then the ring $(A^{\otimes n})^{\mathrm{S}_n}$ is generated as an R-algebra by $\{e_k(a) : k \in \{1, \dots, n\}$ and $a \in \Omega\}$.*

In particular, the Ferrand homomorphism $\Phi_{A/R} \colon (A^{\otimes n})^{\mathrm{S}_n} \to R$ is the unique R-algebra homomorphism sending $e_k(a) \mapsto s_k(a)$ for all $k \in \{1, \dots, n\}$ and $a \in \Omega$. (Note: in case Ω is the set of primitive monomials of a set of algebra generators for A, Lemma 3.6 is a corollary of [17, Theorem 4.10] by an argument similar to the proof of Lemma 3.4.)

Proof. First note that for each $m \in \mathbb{N}$ and $a \in \Omega$, we can express each $e_k(a^m)$ as a polynomial in $\{e_j(a) : j \in \{1, \dots, n\}\}$ by the fundamental theorem of symmetric polynomials. Therefore by adding to Ω all powers of its elements, we can assume without loss of generality that Ω is a set of R-module generators for A that contains 1. Therefore the set $\{\gamma^\alpha(\Omega) : \alpha \in \Omega^n/\mathrm{S}_n\}$ generates $(A^{\otimes n})^{\mathrm{S}_n}$ as an R-module, where we regard Ω as a family of elements of A indexed by itself.

Next we show by induction on k that if $\alpha \in \Omega^n/\mathrm{S}_n$ is the S_n-orbit of any tuple with at most k entries not equal to 1, then $\gamma^\alpha(\Omega)$ is in the subalgebra of $(A^{\otimes n})^{\mathrm{S}_n}$ generated by $\{e_j(a) : a \in \Omega \text{ and } j \in \{1, \dots, k\}\}$. The case $k = n$ then implies that the subalgebra generated by all the $e_k(a)$ contains a set of R-module generators for $(A^{\otimes n})^{\mathrm{S}_n}$, and thus is all of $(A^{\otimes n})^{\mathrm{S}_n}$.

The base case $k = 0$ is clear: if $\alpha = \{(1, \dots, 1)\}$, then $\gamma^\alpha(\Omega) = 1$ is in every subalgebra of $(A^{\otimes n})^{\mathrm{S}_n}$.

Now assume that the hypothesis holds for all $j < k$, and consider an element of the form $\gamma^\alpha(\Omega)$ where α is the S_n-orbit of a tuple in Ω^n with at most k components unequal to 1. Given $a \in \Omega$, let $\alpha(a)$ be the number of times a appears in any single tuple in α; thus $\alpha(1) \geq n - k$ and $\sum_{a \in \Omega \setminus \{1\}} \alpha(a) \leq k$. Construct the element

$$p = \prod_{a \in \Omega \setminus \{1\}} e_{\alpha(a)}(a) \in (A^{\otimes n})^{\mathrm{S}_n};$$

since $\alpha(a) = 0$ (and thus $e_{\alpha(a)}(a) = 1$) for all but finitely many $a \in \Omega$, this product is well-defined. Rewrite the product p as follows: first simplify the product and collect terms related by permutations to write p as a sum of terms of the form $\gamma^{\beta}(A)$, one of which is the original $\gamma^{\alpha}(\Omega)$. For the remainder of the terms, choose an expression of each tensor factor as an R-linear combination of elements of Ω, taking care to choose the same expression each time the same element of A appears and to leave each tensor factor 1 alone. After collecting like terms again, we have written p as $\gamma^{\alpha}(\Omega)$ plus an R-linear combination of terms of the form $\gamma^{\beta}(\Omega)$. These other β all have the property that $\beta(1) > n-k$, so by the induction hypothesis $\gamma^{\alpha}(a) - p$ is in the algebra generated by $\{e_j(a) : a \in \Omega \text{ and } j < k\}$. Therefore $\gamma^{\alpha}(a)$ is in the subalgebra generated by $\{e_j(a) : a \in \Omega \text{ and } j \leq k\}$, as desired. □

For example, given a tuple $a = (a_1, \ldots, a_n)$ of elements of an algebra A, we have the following elements of $A^{\otimes n}$:

$$\gamma^{\mathrm{A}_n}(a) = \sum_{\sigma \in \mathrm{S}_n \text{ even}} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(n)} \text{ and}$$
$$\gamma^{\overline{\mathrm{A}}_n}(a) = \sum_{\sigma \in \mathrm{S}_n \text{ odd}} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(n)},$$

where $\overline{\mathrm{A}}_n$ is the nontrivial coset of A_n, and their sum

$$\gamma^{\mathrm{S}_n}(a) = \sum_{\sigma \in \mathrm{S}_n} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(n)}.$$

Finally, we write the product of two elements of the form $\gamma^G(a_1, \ldots, a_n)$ in terms of more elements of this form.

Lemma 3.7. *Let R be a ring and A an R-algebra. Let n be a natural number and G a subgroup of S_n. Then for each pair of tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ in A^n, the equation*

$$\gamma^G(a)\gamma^G(b) = \sum_{\sigma \in G} \gamma^G(a_1 b_{\sigma(1)}, \ldots, a_n b_{\sigma(n)}).$$

holds in $(A^{\otimes n})^G$.

If we denote the tuple $(b_{\sigma(1)}, \ldots, b_{\sigma(n)})$ by $b_\sigma \in A^n$, and give A^n the product algebra structure, then the product ab_σ is $(a_1 b_{\sigma(1)}, \ldots, a_n b_{\sigma(n)})$, and we may write the above identity as

$$\gamma^G(a)\gamma^G(b) = \sum_{\sigma \in G} \gamma^G(ab_\sigma).$$

Proof. By definition $\gamma^G(a)$ equals $\sum_{\tau \in G} \prod_{i=1}^n a_{\tau(i)}^{(i)}$—recalling the ${}^{(i)}$ notation for the ith embedding $A \to A^{\otimes n}$—so we have

$$\gamma^G(a)\gamma^G(b) = \left(\sum_{\tau \in G} \prod_{i=1}^{n} a_{\tau(i)}^{(i)}\right) \left(\sum_{\sigma \in G} \prod_{i=1}^{d} b_{\sigma(i)}^{(i)}\right).$$

Expanding the product we get

$$\sum_{\tau\in G}\sum_{\sigma\in G}\prod_{i=1}^{n} a^{(i)}_{\tau(i)}b^{(i)}_{\sigma(i)} = \sum_{\tau\in G}\sum_{\sigma\in G}\prod_{i=1}^{n} a^{(i)}_{\tau(i)}b^{(i)}_{\sigma\tau(i)}$$

since for fixed τ the composite $\sigma\tau$ runs over G as σ does. Now $a^{(i)}_{\tau(i)}b^{(i)}_{\sigma\tau(i)} = (ab_\sigma)^{(i)}_{\tau(i)}$, so by reversing the order of summation we find

$$\gamma^G(a)\gamma^G(b) = \sum_{\sigma\in G}\sum_{\tau\in G}\prod_{i=1}^{n}(ab_\sigma)^{(i)}_{\tau(i)} = \sum_{\sigma\in G}\gamma^G(ab_\sigma)$$

as desired. □

4. Proof of Theorem 1

Recall that given a ring R with a rank-$n \geq 2$ algebra A, the discriminant algebra of A (over R) is defined to be the tensor product

$$\Delta_A = (A^{\otimes n})^{\mathrm{A}_n} \bigotimes_{(A^{\otimes n})^{\mathrm{S}_n}} R,$$

using the two ring homomorphisms $(A^{\otimes n})^{\mathrm{S}_n} \hookrightarrow (A^{\otimes n})^{\mathrm{A}_n}$ and the Ferrand homomorphism $\Phi_A \colon (A^{\otimes n})^{\mathrm{S}_n} \to R$. Equivalently, since the Ferrand homomorphism is surjective, we could present Δ_A as the quotient of $(A^{\otimes n})^{\mathrm{A}_n}$ by the ideal generated by elements of the form $\{x - \Phi_A(x) : x \in (A^{\otimes n})^{\mathrm{S}_n}\}$.
In this section, we prove Theorem 1 in the following form:

Theorem 4.1. *Let R be a ring, and let A be an R-algebra of rank n, with $n \geq 2$.*

- *(a) Its discriminant algebra Δ_A fits naturally into a short exact sequence of R-modules*

$$0 \longrightarrow R \longrightarrow \Delta_A \longrightarrow \textstyle\bigwedge^n A \longrightarrow 0.$$

  In particular, Δ_A is an R-algebra of rank 2.
- *(b) The resulting composition of isomorphisms $\bigwedge^n A \cong \Delta_A/(R\cdot 1) \cong \bigwedge^2 \Delta_A$ identifies the discriminant bilinear forms of A and Δ_A.*

In fact, if we denote for each $(a_1, \ldots, a_n) \in A^n$ the image of the A_n-invariant tensor

$$\gamma^{\mathrm{A}_n}(a_1, \ldots, a_n) := \sum_{\sigma\in \mathrm{A}_n} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(n)},$$

under the surjection $(A^{\otimes n})^{\mathrm{A}_n} \twoheadrightarrow \Delta_A$ by $\dot\gamma^{\mathrm{A}_n}(a_1, \ldots, a_n)$, then we can describe the R-module homomorphism $\Delta_A \to \bigwedge^n A$ in the exact sequence as the unique one sending 1 to 0 and each $\dot\gamma^{\mathrm{A}_n}(a_1, \ldots, a_n)$ to $a_1 \wedge \cdots \wedge a_n$. The isomorphism $\bigwedge^n A \cong \bigwedge^2 \Delta_A$ then sends $a_1 \wedge \cdots \wedge a_n$ to $1 \wedge \dot\gamma^{\mathrm{A}_n}(a_1, \ldots, a_n)$.
The outline of the proof of Theorem 4.1(a) is as follows. We show first that the $(A^{\otimes n})^{\mathrm{S}_n}$-linear map $A^{\otimes n} \to (A^{\otimes n})^{\mathrm{A}_n}$ sending $a_1 \otimes \cdots \otimes a_n$ to

$\gamma^{\mathrm{A}_n}(a_1,\dots,a_n)$ descends to an isomorphism of their quotient modules $\bigwedge^n A \cong (A^{\otimes n})^{\mathrm{A}_n}/(A^{\otimes n})^{\mathrm{S}_n}$. This gives us a short exact sequence:

$$0 \longrightarrow (A^{\otimes n})^{\mathrm{S}_n} \longrightarrow (A^{\otimes n})^{\mathrm{A}_n} \longrightarrow \bigwedge^n A \longrightarrow 0.$$

Then we show that base changing this exact sequence along the Ferrand homomorphism $\Phi_{A/R}\colon (A^{\otimes n})^{\mathrm{S}_n} \to R$ gives us the desired exact sequence of R-modules in Theorem 4.1(a). The following lemma gives the technical results needed to make this argument go through.

Lemma 4.2. *Let R be a ring and A an R-algebra of rank $n \geq 2$.*

(1) The R-linear map $A^{\otimes n} \to (A^{\otimes n})^{\mathrm{A}_n}$ sending $a_1 \otimes \cdots \otimes a_n$ to $\gamma^{\mathrm{A}_n}(a_1,\dots,a_n)$ descends to an isomorphism $\bigwedge^n A \cong (A^{\otimes n})^{\mathrm{A}_n}/(A^{\otimes n})^{\mathrm{S}_n}$. In particular, $\bigwedge^n A$ inherits an $(A^{\otimes n})^{\mathrm{S}_n}$-module structure from $A^{\otimes n}$.

(2) The resulting homomorphism from $(A^{\otimes n})^{\mathrm{S}_n}$ to $\mathrm{End}_R(\bigwedge^n A) \cong R$ is the Ferrand homomorphism $\Phi_{A/R}$.

Proof. (1) The R-module homomorphism $A^{\otimes n} \to (A^{\otimes n})^{\mathrm{A}_n}$ sending $a_1\otimes\cdots\otimes a_n$ to $\gamma^{\mathrm{A}_n}(a_1,\dots,a_n)$ is well-defined since $\gamma^{\mathrm{A}_n}(a_1,\dots,a_n)$ is R-linear in each a_i. It is also easily seen to be $(A^{\otimes n})^{\mathrm{S}_n}$-linear. Therefore we obtain an $(A^{\otimes n})^{\mathrm{S}_n}$-module homomorphism $A^{\otimes n} \to (A^{\otimes n})^{\mathrm{A}_n}/(A^{\otimes n})^{\mathrm{S}_n}$ sending $a_1 \otimes \cdots \otimes a_n$ to the class of $\gamma^{\mathrm{A}_n}(a_1,\dots,a_n)$. But if any $a_i = a_j$ with $i \neq j$, we find that $\gamma^{\mathrm{A}_n}(a_1,\dots,a_n)$ is S_n-invariant and thus equal to zero in the quotient. Thus we obtain a well-defined R-module homomorphism

$$\bigwedge^n A \to (A^{\otimes n})^{\mathrm{A}_n}/(A^{\otimes n})^{\mathrm{S}_n}$$

sending $a_1 \wedge \cdots \wedge a_n$ to the class of $\gamma^{\mathrm{A}_n}(a_1,\dots,a_n)$.
Since both sides commute with localization (see Proposition 3.5 for the right-hand side), it suffices to check that this homomorphism is an isomorphism in the case that A is free as an R-module, say with basis $(\theta_1,\dots,\theta_n)$. Then $\bigwedge^n A$ is free with singleton basis $\theta_1\wedge\cdots\wedge\theta_n$. Applying Lemma 3.4, we also find that

$$(A^{\otimes n})^{\mathrm{A}_n} = \bigoplus_{\alpha\in\{1,\dots,n\}^n/\mathrm{A}_n} R\cdot\gamma^\alpha(\theta) \qquad \text{and} \qquad (A^{\otimes n})^{\mathrm{S}_n} = \bigoplus_{\alpha\in\{1,\dots,n\}^n/\mathrm{S}_n} R\cdot\gamma^\alpha(\theta).$$

Now any A_n-orbit of a tuple with a repeated index is actually its S_n-orbit, so these bases are identical except that one uses $\gamma^{\mathrm{A}_n}(\theta)$ and $\gamma^{\overline{\mathrm{A}}_n}(\theta)$, and the other their sum $\gamma^{\mathrm{S}_n}(\theta)$. Thus the quotient is

$$(A^{\otimes n})^{\mathrm{A}_n}/(A^{\otimes n})^{\mathrm{S}_n} = \frac{R\cdot\gamma^{\mathrm{A}_n}(\theta)\oplus R\cdot\gamma^{\overline{\mathrm{A}}_n}(\theta)}{R\cdot(\gamma^{\mathrm{A}_n}(\theta)+\gamma^{\overline{\mathrm{A}}_n}(\theta))},$$

for which we may take either the class of $\gamma^{\mathrm{A}_n}(\theta)$ or $\gamma^{\overline{\mathrm{A}}_n}(\theta)$ as a singleton R-module basis. Then under the homomorphism $\bigwedge^n A \to (A^{\otimes n})^{\mathrm{A}_n}/(A^{\otimes n})^{\mathrm{S}_n}$, the free R-module generator $\theta_1\wedge\cdots\wedge\theta_n$ for $\bigwedge^n A$ is transformed into the class of $\gamma^{\mathrm{A}_n}(\theta_1,\dots,\theta_n)$, which we now know to also be a free R-module generator for $(A^{\otimes n})^{\mathrm{A}_n}/(A^{\otimes n})^{\mathrm{S}_n}$.

(2) We check the defining property of the Ferrand homomorphism. First, let $a \in A$; we will see which endomorphism of $\bigwedge^n A$ the element $a \otimes \cdots \otimes a \in (A^{\otimes n})^{\mathrm{S}_n}$ gives rise to. The $(A^{\otimes n})^{\mathrm{S}_n}$-module structure on $\bigwedge^n A$ is the one inherited from the $(A^{\otimes n})^{\mathrm{S}_n}$-algebra $A^{\otimes n}$, so the endomorphism of $\bigwedge^n A$ corresponding to $a \otimes \cdots \otimes a$ is

$$b_1 \wedge \cdots \wedge b_n \mapsto (ab_1) \wedge \cdots \wedge (ab_n).$$

But by definition, this endomorphism is multiplication by $\mathrm{Nm}_{A/R}(a) \in R$, as desired.

Now we check that for each R-algebra R', if we set $A' = R' \otimes_R A$ then the base-changed homomorphism

$$(A'^{\otimes_{R'} n})^{\mathrm{S}_n} \cong R' \otimes_R (A^{\otimes n})^{\mathrm{S}_n} \to R' \otimes_R \mathrm{End}_R(\textstyle\bigwedge^n A) \cong \mathrm{End}_{R'}(\textstyle\bigwedge^n A')$$

has the same property, sending each $a \otimes \cdots \otimes a$ to multiplication by $\mathrm{Nm}_{A'/R'}(a) \in R'$. But this follows because the base-changed homomorphism is again the one expressing the fact that $\bigwedge^n A'$ inherits an $(A'^{\otimes_{R'} n})^{\mathrm{S}_n}$-module structure from $A'^{\otimes_{R'} n}$. $\square$

Proof of Theorem 4.1(a). By Lemma 4.2(1), we obtain a short exact sequence of $(A^{\otimes n})^{\mathrm{S}_n}$-modules

$$0 \to (A^{\otimes n})^{\mathrm{S}_n} \to (A^{\otimes n})^{\mathrm{A}_n} \to \textstyle\bigwedge^n A \to 0$$

where the right-hand map sends $\gamma^{\mathrm{A}_n}(a_1, \ldots, a_n) \mapsto a_1 \wedge \cdots \wedge a_n$. Tensoring along the Ferrand homomorphism $\Phi_{A/R} \colon (A^{\otimes n})^{\mathrm{S}_n} \to R$ is equivalent to quotienting by its kernel $I = (x - \Phi_A(x) : x \in (A^{\otimes n})^{\mathrm{S}_n})$, obtaining an *a priori* merely right-exact sequence

$$(A^{\otimes n})^{\mathrm{S}_n}/I \to (A^{\otimes n})^{\mathrm{A}_n}/\big(I \cdot (A^{\otimes n})^{\mathrm{A}_n}\big) \to \textstyle\bigwedge^n A/\big(I \cdot \bigwedge^n A\big) \to 0.$$

From left to right, these modules are R, Δ_A, and $\bigwedge^n A$, in the latter case because I, being the kernel of the Ferrand homomorphism, is also the annihilator of the $(A^{\otimes n})^{\mathrm{S}_n}$-module $\bigwedge^n A$ by Lemma 4.2(2). Thus we have a right exact sequence of R-modules

$$R \to \Delta_A \to \textstyle\bigwedge^n A \to 0,$$

where the left-hand map sends $1 \mapsto 1$ and the right-hand map sends each $\dot\gamma^{\mathrm{A}_n}(a_1, \ldots, a_n)$ to $a_1 \wedge \cdots \wedge a_n$. But then $R \to \Delta_A$ must be injective: if $r \mapsto 0$, then r acts by zero on Δ_A and hence on its quotient $\bigwedge^n A$. But then r must be zero, since $\bigwedge^n A$ is locally free of rank 1 and thus a faithful R-module.

(Another way to see that $R \to \Delta_A$ is injective is to note that I is the annihilator of the $(A^{\otimes n})^{\mathrm{S}_n}$-module $(A^{\otimes n})^{\mathrm{A}_n}/(A^{\otimes n})^{\mathrm{S}_n}$. It is thus the largest ideal of $(A^{\otimes n})^{\mathrm{S}_n}$ whose product with $(A^{\otimes n})^{\mathrm{A}_n}$ is contained in $(A^{\otimes n})^{\mathrm{S}_n}$; therefore $I \cdot (A^{\otimes n})^{\mathrm{A}_n} = I$. Thus the map $R \to \Delta_A$ is the map

$$(A^{\otimes n})^{\mathrm{S}_n}/I \to (A^{\otimes n})^{\mathrm{A}_n}/\big(I \cdot (A^{\otimes n})^{\mathrm{A}_n}\big) = (A^{\otimes n})^{\mathrm{A}_n}/I,$$

which is manifestly injective.) $\square$

The remainder of the section is devoted to proving Theorem 4.1(b). Our first result relates the multiplication of some elements of Δ_A to the discriminant form of A.

Lemma 4.3. *Let R be a ring. Let A be an R-algebra of rank $n \geq 2$. Let $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ be in A^n. Then the equality*

$$\big(\dot\gamma^{\mathrm{A}_n}(a) - \dot\gamma^{\overline{\mathrm{A}}_n}(a)\big)\big(\dot\gamma^{\mathrm{A}_n}(b) - \dot\gamma^{\overline{\mathrm{A}}_n}(b)\big) = \delta_A(a_1 \wedge \cdots \wedge a_n, b_1 \wedge \cdots \wedge b_n)$$

holds in Δ_A.

Proof. Recall fromm Eq. (2) at the beginning of Section 3 the notation $(\cdot)^{(i)}$ for the ith embedding $A \to A^{\otimes n}$. Then we may write the difference $\gamma^{\mathrm{A}_n}(a) - \gamma^{\overline{\mathrm{A}}_n}(a)$ in $A^{\otimes n}$ as

$$\sum_{\sigma \in \mathrm{A}_n} \prod_{i=1}^{n} a_i^{(\sigma(i))} - \sum_{\sigma \in \overline{\mathrm{A}}_n} \prod_{i=1}^{n} a_i^{(\sigma(i))} = \sum_{\sigma \in \mathrm{S}_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_i^{(\sigma(i))},$$

the determinant of the $n \times n$-matrix whose ijth element is $a_i^{(j)}$, and similarly $\gamma^{\mathrm{A}_n}(b) - \gamma^{\overline{\mathrm{A}}_n}(b) = \det\big(b_k^{(j)}\big)_{jk}$. From this, we can write

$$\begin{aligned}\big(\gamma^{\mathrm{A}_n}(a) - \gamma^{\overline{\mathrm{A}}_n}(a)\big)\big(\gamma^{\mathrm{A}_n}(b) - \gamma^{\overline{\mathrm{A}}_n}(b)\big) &= \det\big(a_i^{(j)}\big)_{ij} \det\big(b_k^{(j)}\big)_{jk} \\ &= \det\Big(\sum_{j=1}^{n} a_i^{(j)} b_k^{(j)}\Big)_{ik}.\end{aligned}$$

The symbol $a_i^{(j)} b_k^{(j)}$ is equal to $(a_i b_k)^{(j)}$, and the sum over all j gives by definition $e_1(a_i b_k)$. This is in $(A^{\otimes n})^{\mathrm{S}_n}$ and by Lemma 3.1 its image under the Ferrand homomorphism is $s_1(a_i b_k) = \mathrm{Tr}_A(a_i b_k)$. Hence in Δ_A we have

$$\begin{aligned}\big(\dot\gamma^{\mathrm{A}_n}(a) - \dot\gamma^{\overline{\mathrm{A}}_n}(a)\big)\big(\dot\gamma^{\mathrm{A}_n}(b) - \dot\gamma^{\overline{\mathrm{A}}_n}(b)\big) &= \det\big(\mathrm{Tr}_A(a_i b_k)\big)_{ik} \\ &= \delta_A(a_1 \wedge \cdots \wedge a_n, b_1 \wedge \cdots \wedge b_n)\end{aligned}$$

as we wanted to show. □

For comparing the discriminant form of Δ_A with that of A, we will need to understand the trace map $\mathrm{Tr}_{\Delta_A} \colon \Delta_A \to R$. A helpful intermediate step is to understand the so-called standard involution on any rank-2 algebra:

Definition 4.4. Let R be a ring and D an R-algebra of rank 2. The function $\tau_D \colon D \to D$ sending $d \mapsto \mathrm{Tr}_D(d) - d$ is called the *standard involution* on D, and has the property that

$$d + \tau_D(d) = \mathrm{Tr}_D(d) \text{ and } d \cdot \tau_D(d) = \mathrm{Nm}_D(d)$$

for all $d \in D$. It is in fact an involution and an R-algebra homomorphism, and is even the unique R-algebra involution $\tau \colon D \to D$ such that $d \cdot \tau(d) \in R$ for all $d \in D$ (see, for example, [18, Lemma 2.9]).

Corollary 4.5. *Let R be a ring and A an R-algebra of rank n, with $n \geq 2$. Let τ be the map $\Delta_A \to \Delta_A$ induced by the action of a transposition on the tensor factors in $(A^{\otimes n})^{\mathrm{A}_n}$. Then τ is the standard involution on Δ_A.*

Proof. Since the action of a transposition on any S_n-invariant element is trivial, the map $\tau\colon \Delta_A \to \Delta_A$ is a well-defined R-algebra involution on Δ_A. And for any element x of $(A^{\otimes n})^{\mathrm{A}_n}$, we have that $x \cdot \tau(x)$ is S_n-invariant, and so is sent to an element of R in Δ_A. Therefore τ is indeed the standard involution on Δ_A. □

We can now prove that the exact sequence of Theorem 4.1 identifies the discriminant forms of A and Δ_A.

Proof of Theorem 4.1(b). The composite isomorphism $\bigwedge^n A \cong \Delta_A/R \cong \bigwedge^2 \Delta_A$ sends an element $a_1 \wedge \cdots \wedge a_n$ of $\bigwedge^n A$ to $1 \wedge \dot\gamma^{\mathrm{A}_n}(a_1, \ldots, a_n)$ in $\bigwedge^2 \Delta_A$. Given $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in A^n we have

$$\delta_{\Delta_A}\big(1 \wedge \dot\gamma^{\mathrm{A}_n}(a), 1 \wedge \dot\gamma^{\mathrm{A}_n}(b)\big) = \det \begin{pmatrix} \mathrm{Tr}_{\Delta_A}(1) & \mathrm{Tr}_{\Delta_A}\big(\dot\gamma^{\mathrm{A}_n}(b)\big) \\ \mathrm{Tr}_{\Delta_A}\big(\dot\gamma^{\mathrm{A}_n}(a)\big) & \mathrm{Tr}_{\Delta_A}\big(\dot\gamma^{\mathrm{A}_n}(a)\dot\gamma^{\mathrm{A}_n}(b)\big) \end{pmatrix}$$

which is equal to

$$2\mathrm{Tr}_{\Delta_A}(\dot\gamma^{\mathrm{A}_n}(a)\dot\gamma^{\mathrm{A}_n}(b)) - \mathrm{Tr}_{\Delta_A}(\dot\gamma^{\mathrm{A}_n}(a))\mathrm{Tr}_{\Delta_A}(\dot\gamma^{\mathrm{A}_n}(b)).$$

By Corollary 4.5, the standard involution of Δ_A is the one arising from the action of a transposition on the tensor factors of $A^{\otimes n}$, so we may compute these traces as sums:

$$\begin{aligned} \delta_{\Delta_A}(1 \wedge \dot\gamma^{\mathrm{A}_n}(a), 1 \wedge \dot\gamma^{\mathrm{A}_n}(b)) &= 2\big(\dot\gamma^{\mathrm{A}_n}(a)\dot\gamma^{\mathrm{A}_n}(b) + \dot\gamma^{\overline{\mathrm{A}}_n}(a)\dot\gamma^{\overline{\mathrm{A}}_n}(b)\big) \\ &\quad - \big(\dot\gamma^{\mathrm{A}_n}(a) + \dot\gamma^{\overline{\mathrm{A}}_n}(a)\big)\big(\dot\gamma^{\mathrm{A}_n}(b) + \dot\gamma^{\overline{\mathrm{A}}_n}(b)\big) \\ &= \big(\dot\gamma^{\mathrm{A}_n}(a) - \dot\gamma^{\overline{\mathrm{A}}_n}(a)\big)\big(\dot\gamma^{\mathrm{A}_n}(b) - \dot\gamma^{\overline{\mathrm{A}}_n}(b)\big) \end{aligned}$$

which is equal to $\delta_A(a_1 \wedge \cdots \wedge a_n, b_1 \wedge \cdots \wedge b_n)$ by Lemma 4.3. So the given isomorphism identifies the discriminant forms of A and Δ_A, as we wanted to show. □

5. Examples of discriminant algebras

To show that computing Δ_A for A an algebra of rank n is a straightforward process, in this section we will exhibit some examples of discriminant algebras and how to compute them. The simplest case, the discriminant algebra of a quadratic (i.e. rank-2) algebra, is reassuring but not very illuminating.

PROPOSITION 5.1. *Let R be a ring and A a quadratic R-algebra. Then the R-algebra homomorphism $A \to \Delta_A$ sending $a \mapsto \dot\gamma^{\mathrm{A}_2}(1, a)$ is an isomorphism.*

Proof. That this is an R-algebra homomorphism is evident from its factorization as

$$A \to A^{\otimes 2} = (A^{\otimes 2})^{\mathrm{A}_2} \to \Delta_A$$

sending $a \mapsto 1 \otimes a = \gamma^{\mathrm{A}_2}(1,a) \mapsto \dot\gamma^{\mathrm{A}_2}(1,a)$. That it is an isomorphism then follows by the Five Lemma from the following commuting diagram:

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r] \arrow[d, equal] & A \arrow[r] \arrow[d] & \bigwedge^2 A \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & R \arrow[r] & \Delta_A \arrow[r] & \bigwedge^2 A \arrow[r] & 0, \end{tikzcd}$$

where the bottom row is the short exact sequence of Theorem 4.1, and the map $A \to \bigwedge^2 A$ in the top row sends a to $1 \wedge a$. The left-hand square commutes because $A \to \Delta_A$ is an R-algebra homomorphism, and the right-hand square commutes because the composite $A \to \Delta_A \to \bigwedge^2 A$ also sends $a \mapsto \dot\gamma^{\mathrm{A}_2}(1,a) \mapsto 1 \wedge a$. $\square$

The simplest non-trivial example of a discriminant algebra will therefore be that of a rank-3 algebra. The following proposition is quite useful for computing discriminant algebras of algebras that are free as modules.

Proposition 5.2. *Let R be a ring, and suppose A is an R-algebra that is free of rank $n \geq 2$ as an R-module, with R-basis $\theta = (\theta_1, \dots, \theta_n)$. Then Δ_A is also free as an R-module, with R-basis $\{1, \dot\gamma^{\mathrm{A}_n}(\theta)\}$.*

Proof. Note that if A is free with R-basis $(\theta_1, \dots, \theta_n)$, then $\bigwedge^n A$ is free of rank 1, with generator $\theta_1 \wedge \cdots \wedge \theta_n$. Then from the exact sequence of Theorem 4.1, we find that $\{1, \dot\gamma^{\mathrm{A}_n}(\theta)\}$ is an R-basis for Δ_A, because it is the disjoint union of an R-basis for R and a lifting of an R-basis for $\bigwedge^n A$. $\square$

Remark 5.3. More generally, if $\Theta \subseteq A^n$ is a set of tuples such that

$$\{\theta_1 \wedge \cdots \wedge \theta_n : (\theta_1, \dots, \theta_n) \in \Theta\}$$

generates $\bigwedge^n A$ as an R-module, then Δ_A is generated as an R-module by 1 together with

$$\{\dot\gamma^{\mathrm{A}_n}(\theta_1, \dots, \theta_n) : (\theta_1, \dots, \theta_n) \in \Theta\}.$$

Remark 5.4. In the setting of Proposition 5.2, note that since $\dot\gamma^{\mathrm{A}_n}(\theta)$ has trace $\dot\gamma^{\mathrm{A}_n}(\theta) + \dot\gamma^{\overline{\mathrm{A}}_n}(\theta)$ and norm $\dot\gamma^{\mathrm{A}_n}(\theta)\dot\gamma^{\overline{\mathrm{A}}_n}(\theta)$ by Corollary 4.5, we find that

$$\Delta_A \cong R[X]/(X^2 - (\dot\gamma^{\mathrm{A}_n}(\theta) + \dot\gamma^{\overline{\mathrm{A}}_n}(\theta))X + (\dot\gamma^{\mathrm{A}_n}(\theta)\dot\gamma^{\overline{\mathrm{A}}_n}(\theta))).$$

Note that this quadratic polynomial in X has discriminant

$$\begin{aligned} \big(\dot\gamma^{\mathrm{A}_n}(\theta) + \dot\gamma^{\overline{\mathrm{A}}_n}(\theta)\big)^2 - 4\big(\dot\gamma^{\mathrm{A}_n}(\theta)\dot\gamma^{\overline{\mathrm{A}}_n}(\theta)\big) &= \big(\dot\gamma^{\mathrm{A}_n}(\theta) - \dot\gamma^{\overline{\mathrm{A}}_n}(\theta)\big)^2 \\ &= \delta_A(\theta_1 \wedge \cdots \wedge \theta_n, \theta_1 \wedge \cdots \wedge \theta_n), \end{aligned}$$

the discriminant of A with respect to the basis θ.

As an immediate consequence, we find that the discriminant of A with respect to the R-basis θ is a square in $R/(4)$. This generalizes Stickelberger's theorem that the discriminant of a number field is always congruent to 0 or 1 modulo 4.

Example 5.5. Let R be a ring, and let E be a locally-free R-module of rank $n \geq 1$. Then $R \oplus E$ can be given an R-algebra structure in which $(1,0)$ is the multiplicative identity and E is a square-zero ideal. Its discriminant algebra is then

$$\Delta_{R\oplus E} \cong R \oplus \bigwedge^n E,$$

again with multiplicative identity $(1,0)$ and $\bigwedge^n E$ a square-zero ideal.
We show this by proving that there is a unique R-module homomorphism $\Delta_{R\oplus E} \to R \oplus \bigwedge^n E$ sending $1 \mapsto (1,0)$ and $\dot{\gamma}^{\mathrm{A}_{n+1}}(1,e) := \dot{\gamma}^{\mathrm{A}_{n+1}}(1,e_1,\dots,e_n) \mapsto (0, e_1 \wedge \cdots \wedge e_n)$ for all tuples $e = (e_1,\dots,e_n) \in E^n$. We will then show that this homomorphism is an isomorphism, and that the induced multiplication on $R \oplus \bigwedge^n E$ is the desired one.
Uniqueness is clear, as such elements generate $\Delta_{R\oplus E}$ by Remark 5.3. For existence, then, it suffices to check locally, when E is free with basis $\theta = (\theta_1,\dots,\theta_n)$. Then $\Delta_{R\oplus E}$ is free with basis $\big(1, \dot{\gamma}^{\mathrm{A}_{n+1}}(1,\theta)\big)$ and $R \oplus \bigwedge^n E$ is free with basis $\big((1,0),(0,\theta_1\wedge\cdots\wedge\theta_n)\big)$, so we may define an R-module homomorphism $\Delta_{R\oplus E} \to R \oplus \bigwedge^n E$ sending $1 \mapsto (1,0)$ and

$$\dot{\gamma}^{\mathrm{A}_{n+1}}(1,\theta) \mapsto (0, \theta_1 \wedge \cdots \wedge \theta_n).$$

We claim that this homomorphism has the desired property, that

$$\dot{\gamma}^{\mathrm{A}_{n+1}}(1,e) \mapsto (0, e_1 \wedge \cdots \wedge e_n)$$

for all $e = (e_1,\dots,e_n) \in E^n$. We check this first in case $e = \theta_\sigma$, that is, the e_i are a permutation of the θ_i—see the discussion after Lemma 3.7. If σ is even, then $\dot{\gamma}^{\mathrm{A}_{n+1}}(1,e) = \dot{\gamma}^{\mathrm{A}_{n+1}}(1,\theta)$ and $e_1 \wedge \cdots \wedge e_n = \theta_1 \wedge \cdots \wedge \theta_n$, and we are done. If σ is odd, then $\dot{\gamma}^{\mathrm{A}_{n+1}}(1,e) = \dot{\gamma}^{\overline{\mathrm{A}}_{n+1}}(1,\theta)$, and what we instead must show is that

$$\dot{\gamma}^{\overline{\mathrm{A}}_{n+1}}(1,\theta) \mapsto (0, -\theta_1 \wedge \cdots \wedge \theta_n).$$

We show this by proving that the sum of $\dot{\gamma}^{\mathrm{A}_{n+1}}(1,\theta)$ and $\dot{\gamma}^{\overline{\mathrm{A}}_{n+1}}(1,\theta)$ is zero, and so the image of the latter is the negative of the image of the former.
Now we can compute $\dot{\gamma}^{\mathrm{A}_{n+1}}(1,\theta) + \dot{\gamma}^{\overline{\mathrm{A}}_{n+1}}(1,\theta) = \dot{\gamma}^{\mathrm{S}_{n+1}}(1,\theta) = \Phi_A\big(\gamma^{\mathrm{S}_{n+1}}(1,\theta)\big)$ as the coefficient of $\lambda_0\lambda_1\cdots\lambda_n$ in the norm of $\lambda_0 + \sum_{i=1}^n \lambda_i\theta_i$. This element acts via the following matrix:

$$\begin{pmatrix} \lambda_0 & 0 & 0 & \dots & 0 \\ \lambda_1 & \lambda_0 & 0 & \dots & 0 \\ \lambda_2 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \lambda_0 & 0 \\ \lambda_n & 0 & \dots & 0 & \lambda_0 \end{pmatrix}$$

This matrix is lower-triangular and has λ_0s on the diagonal, so the determinant is λ_0^{n+1}, in which the coefficient of $\lambda_0\lambda_1\cdots\lambda_n$ is zero, as desired. Thus the homomorphism we have defined does indeed send $\dot{\gamma}^{\mathrm{A}_{n+1}}(1,e)$ to $(0, e_1 \wedge \cdots \wedge e_n)$ whenever the e_i are a permutation of the θ_i.

Now we check that this holds for general e. Write $e_i = \sum_j m_{ij}\theta_j$ for some $m_{ij} \in R$. Then we have

$$\begin{aligned}\dot\gamma^{\mathrm{A}_{n+1}}(1,e) &= \dot\gamma^{\mathrm{A}_{n+1}}\Big(1, \sum_{j=1}^n m_{1j}\theta_j, \ldots, \sum_{j=1}^n m_{nj}\theta_j\Big)\\ &= \sum_{f\colon \{1,\ldots,n\}\to\{1,\ldots,n\}} \Big(\prod_{i=1}^n m_{if(i)}\Big)\dot\gamma^{\mathrm{A}_{n+1}}(1,\theta_{f(1)},\ldots,\theta_{f(n)}).\end{aligned}$$

We claim that the terms with f not injective equal zero. Indeed, if f is not injective then $\gamma^{\mathrm{A}_{n+1}}(1,\theta_{f(1)},\ldots,\theta_{f(n)})$ is S_{n+1}-invariant and equals $\gamma^\alpha(1,\theta_1,\ldots,\theta_n)$ for some $\alpha \in \{0,\ldots,n\}^{n+1}/\mathrm{S}_{n+1}$. But then its image in Δ_A is the coefficient of λ^α in the norm of $\lambda_0 + \sum_{i=1}^n \lambda_i\theta_i$, which vanishes unless $\alpha = \{(0,0,\ldots,0)\}$, but this case cannot arise. Therefore

$$\begin{aligned}\dot\gamma^{\mathrm{A}_{n+1}}(1,e) &= \sum_{\sigma\in\mathrm{S}_n}\Big(\prod_{i=1}^n m_{i\sigma(i)}\Big)\dot\gamma^{\mathrm{A}_{n+1}}(1,\theta_{\sigma(1)},\ldots,\theta_{\sigma(n)})\\ &\mapsto (0, \sum_{\sigma\in\mathrm{S}_n}\Big(\prod_{i=1}^n m_{i\sigma(i)}\Big)\mathrm{sgn}(\sigma)\ \theta_1\wedge\cdots\wedge\theta_n)\\ &= (0, \det\big(m_{ij}\big)_{ij}\ \theta_1\wedge\cdots\wedge\theta_n)\\ &= (0, e_1\wedge\cdots\wedge e_n)\end{aligned}$$

as desired. Thus we have an R-module homomorphism $\Delta_{R\oplus E} \to R\oplus\bigwedge^n E$ sending $\dot\gamma^{\mathrm{A}_{n+1}}(1,e)$ to $(0,e_1\wedge\cdots\wedge e_n)$, and since it is an isomorphism locally, it is an isomorphism of R-modules.
Then all that remains to check is that the induced R-algebra structure on $R\oplus\bigwedge^n E$ is the indicated one. Now as long as $n\geq 2$, every term in a product of the form

$$\dot\gamma^{\mathrm{A}_{n+1}}(1,e_1,\ldots,e_n)\dot\gamma^{\mathrm{A}_{n+1}}(1,f_1,\ldots,f_n)$$

vanishes because every product $e_if_j = 0$. Thus the multiplication on $R\oplus\bigwedge^n E$ sets $(e_1\wedge\cdots\wedge e_n)(f_1\wedge\cdots\wedge f_n) = 0$ as desired. If we are in the case $n=1$, then $R\oplus E$ is a rank-2 algebra and we have $\Delta_{R\oplus E}\cong R\oplus E\cong R\oplus\bigwedge^1 E$ anyway.

Example 5.6. Let R be a ring and A be an R-algebra of rank n that can be generated by a single element a. Then if $p_a(\lambda)$ is the characteristic polynomial of a, we have $A\cong R[X]/(p_a(X))$. In particular, $\{1,a,\ldots,a^{n-1}\}$ is an R-basis of A. So we find that $\{1,\dot\gamma^{\mathrm{A}_{n+1}}(1,a,\ldots,a^{n-1})\}$ is an R-basis of Δ_A.
For example, if $n=3$ and $p_a(X) = X^3 - sX^2 + tX - u$, then we have an R-basis for Δ_A given by $\{1,\dot\gamma^{\mathrm{A}_3}(1,a,a^2)\}$. We can compute the trace and norm of the generator $\dot\gamma^{\mathrm{A}_3}(1,a,a^2)$ as follows: for the trace, we need only a small

calculation

$$\begin{aligned}\mathrm{Tr}_{\Delta_A}(\dot\gamma^{\mathrm{A}_3}(1,a,a^2)) &= \Phi_A(\gamma^{\mathrm{S}_3}(1,a,a^2))\\ &= \Phi_A(e_1(a)e_2(a)-3e_3(a))\\ &= s_1(a)s_2(a)-3s_3(a)\\ &= st-3u.\end{aligned}$$

For the norm, we have

$$\begin{aligned}\mathrm{Nm}_{\Delta_A}(\dot\gamma^{\mathrm{A}_3}(1,a,a^2)) &= \dot\gamma^{\mathrm{A}_3}(1,a,a^2)\dot\gamma^{\overline{\mathrm{A}_3}}(1,a,a^2)\\ &= \dot\gamma^{\mathrm{A}_3}(1,a^3,a^3)+\dot\gamma^{\mathrm{A}_3}(a^2,a^2,a^2)+\dot\gamma^{\mathrm{A}_3}(a,a,a^4).\end{aligned}$$

(The reader may check this expansion by hand, or appeal to Lemma 3.7.) We have $\dot\gamma^{\mathrm{A}_3}(a^2,a^2,a^2)=3u^2$, as this is just three times the norm of a^2. Moreover, we have that $\gamma^{\mathrm{A}_3}(a,a,a^4)$ is equal to $e_3(a)\gamma^{\mathrm{A}_3}(1,1,a^3)$ so that $\dot\gamma^{\mathrm{A}_3}(a,a,a^4)=u\dot\gamma^{\mathrm{A}_3}(1,1,a^3)$. Moreover $\dot\gamma^{\mathrm{A}_3}(1,1,a^3)$ and $\dot\gamma^{\mathrm{A}_3}(1,a^3,a^3)$ are equal to $s_1(a^3)$ and $s_2(a^3)$ respectively. Hence, we just need to compute $s_1(a^3)$ and $s_2(a^3)$. The action of a^3 with respect to the basis $(1,a,a^2)$ is given by the matrix

$$\begin{pmatrix}0&0&u\\1&0&-t\\0&1&s\end{pmatrix}^3=\begin{pmatrix}u&su&s^2u-tu\\-t&u-st&su-s^2t+t^2\\s&s^2-t&u-2st+s^3\end{pmatrix},$$

which has trace $s_1(a^3)=3u-3st+s^3$ and quadratic trace $s_2(a^3)=3u^2-3stu+t^3$. So we obtain

$$\begin{aligned}\mathrm{Nm}_{\Delta_A}(\dot\gamma^{\mathrm{A}_3}(1,a,a^2)) &= s_2(a^3)+3u^2+us_1(a^3)\\ &= (3u^2-3stu+t^3)+3u^2+u(3u-3st+s^3)\\ &= 9u^2-6stu+t^3+s^3u.\end{aligned}$$

Therefore we have the following algebra presentation:

$$\Delta_A\cong R[X]/(X^2-(st-3u)X+(9u^2-6stu+t^3+s^3u)).$$

Example 5.7. Consider the cyclotomic extension of rings of integers $\mathbb{Z}[\zeta]\cong\mathbb{Z}[x]/(x^4+x^3+x^2+x+1)$ over $\mathbb{Z}$ for ζ a primitive 5th root of unity. The discriminant of this $\mathbb{Z}$-algebra is

$$\begin{vmatrix}\mathrm{Tr}_K(1)&\mathrm{Tr}_K(\zeta)&\mathrm{Tr}_K(\zeta^2)&\mathrm{Tr}_K(\zeta^3)\\ \mathrm{Tr}_K(\zeta)&\mathrm{Tr}_K(\zeta^2)&\mathrm{Tr}_K(\zeta^3)&\mathrm{Tr}_K(\zeta^4)\\ \mathrm{Tr}_K(\zeta^2)&\mathrm{Tr}_K(\zeta^3)&\mathrm{Tr}_K(\zeta^4)&\mathrm{Tr}_K(1)\\ \mathrm{Tr}_K(\zeta^3)&\mathrm{Tr}_K(\zeta^4)&\mathrm{Tr}_K(1)&\mathrm{Tr}_K(\zeta)\end{vmatrix}=\begin{vmatrix}4&-1&-1&-1\\-1&-1&-1&-1\\-1&-1&-1&4\\-1&-1&4&-1\end{vmatrix}=5^3.$$

Adjoining a square root of the discriminant to $\mathbb{Z}$, we obtain a naive discriminant algebra $\Delta^{\mathrm{naive}}_{O_K/\mathbb{Z}}=\mathbb{Z}[x]/(x^2-125)$. But the discriminant of this quadratic $\mathbb{Z}$-algebra is $(0)^2-4(-125)=2^2\cdot5^3$, which is *not* equivalent to that of $O_K/\mathbb{Z}$, since 2^2 is not the square of a unit in $\mathbb{Z}$.

Let us see instead what our construction $\Delta_{O_K/\mathbb{Z}}$ gives. The $\mathbb{Z}$-basis $\{1,\zeta,\zeta^2,\zeta^3\}$ for $\mathbb{Z}[\zeta]$ gives a basis $\{1,\dot\gamma^{\mathrm{A}_4}(1,\zeta,\zeta^2,\zeta^3)\}$ for the discriminant algebra. We compute the trace and norm of $\dot\gamma^{\mathrm{A}_4}(1,\zeta,\zeta^2,\zeta^3)$ to give a presentation for this algebra:

$$\begin{aligned}\mathrm{Tr}_{\Delta_{\mathbb{Z}[\zeta]}}\big(\dot\gamma^{\mathrm{A}_4}(1,\zeta,\zeta^2,\zeta^3)\big) &= \dot\gamma^{\mathrm{A}_4}(1,\zeta,\zeta^2,\zeta^3)+\dot\gamma^{\overline{\mathrm{A}}_4}(1,\zeta,\zeta^2,\zeta^3)\\ &= \Phi_{\mathbb{Z}[\zeta]}\big(\gamma^{\mathrm{S}_4}(1,\zeta,\zeta^2,\zeta^3)\big),\end{aligned}$$

which the algorithm in Lemma 3.6 expresses as

$$\begin{aligned}&\Phi_{\mathbb{Z}[\zeta]}\big(e_1(\zeta)e_1(\zeta^2)e_1(\zeta^3)-e_1(\zeta)e_1(\zeta^5)-e_1(\zeta^2)e_1(\zeta^4)-2e_2(\zeta^3)+e_1(\zeta^6)\big)\\ &\quad= s_1(\zeta)s_1(\zeta^2)s_1(\zeta^3)-s_1(\zeta)s_1(\zeta^5)-s_1(\zeta^2)s_1(\zeta^4)-2s_2(\zeta^3)+s_1(\zeta^6)\\ &\quad= (-1)(-1)(-1)-(-1)(4)-(-1)(-1)-2(1)+(-1)\\ &\quad= -1+4-1-2-1=-1.\end{aligned}$$

The norm we compute with the help of Lemma 3.7:

$$\begin{aligned}\mathrm{Nm}_{\Delta_{\mathbb{Z}[\zeta]}}\big(\dot\gamma^{\mathrm{A}_4}(1,\zeta,\zeta^2,\zeta^3)\big) &= \dot\gamma^{\mathrm{A}_4}(1,\zeta,\zeta^2,\zeta^3)\dot\gamma^{\overline{\mathrm{A}}_4}(1,\zeta,\zeta^2,\zeta^3)\end{aligned}$$
$$\begin{array}{rlrl} = & \dot\gamma^{\mathrm{A}_4}(\zeta,\zeta,\zeta^4,\zeta) & + & \dot\gamma^{\mathrm{A}_4}(\zeta,\zeta^2,1,\zeta^4)\\ + & \dot\gamma^{\mathrm{A}_4}(\zeta,\zeta^3,\zeta^3,1) & + & \dot\gamma^{\mathrm{A}_4}(\zeta^2,1,1,1)\\ + & \dot\gamma^{\mathrm{A}_4}(\zeta^2,\zeta^2,\zeta^2,\zeta) & + & \dot\gamma^{\mathrm{A}_4}(\zeta^2,\zeta^3,\zeta^4,\zeta^3)\\ + & \dot\gamma^{\mathrm{A}_4}(\zeta^3,1,\zeta^3,\zeta) & + & \dot\gamma^{\mathrm{A}_4}(\zeta^3,\zeta,1,\zeta^3)\\ + & \dot\gamma^{\mathrm{A}_4}(\zeta^3,\zeta^3,\zeta^2,\zeta^4) & + & \dot\gamma^{\mathrm{A}_4}(\zeta^4,1,\zeta^4,\zeta^4)\\ + & \dot\gamma^{\mathrm{A}_4}(\zeta^4,\zeta,\zeta^2,1) & + & \dot\gamma^{\mathrm{A}_4}(\zeta^4,\zeta^2,\zeta^3,\zeta^3).\end{array}$$

Each term with a repeated entry is easy to expand in terms of the $s_k(\zeta^j)$; for example:

$$\dot\gamma^{\mathrm{A}_4}(\zeta,\zeta,\zeta^4,\zeta)=s_4(\zeta)\dot\gamma^{\mathrm{A}_4}(1,1,\zeta^3,1)=3s_4(\zeta)s_1(\zeta^3)=3(1)(-1)=-3$$

and

$$\begin{aligned}\dot\gamma^{\mathrm{A}_4}(\zeta,\zeta^3,\zeta^3,1) &= s_1(\zeta)s_2(\zeta^3)-s_1(\zeta^3)s_1(\zeta^4)+s_1(\zeta^7)\\ &= (-1)(1)-(-1)(-1)+(-1)=-3.\end{aligned}$$

In fact, all the terms equal -3 except for $\dot\gamma^{\mathrm{A}_4}(\zeta,\zeta^2,1,\zeta^4)$ and $\dot\gamma^{\mathrm{A}_4}(\zeta^4,\zeta,\zeta^2,1)$, whose sum when multiplied by $s_4(\zeta)=1$ gives $\mathrm{Tr}\big(\dot\gamma^{\mathrm{A}_4}(\zeta^2,\zeta^3,\zeta,1)\big)=-1$. Thus the trace and norm of $\dot\gamma^{\mathrm{A}_4}(1,\zeta,\zeta^2,\zeta^3)$ are -1 and $10(-3)-1=-31$, so

$$\Delta_{O_K/\mathbb{Z}}\cong\mathbb{Z}[x]/(x^2+x-31),$$

which does have discriminant $(1)^2-4(-31)=125$ equal to that of O_K.

While theoretically well-behaved, sometimes the coefficients in a presentation of the discriminant algebra are hard to interpret.

Example 5.8. Let A be the rank-n $\mathbb{Z}$-algebra $\mathbb{Z}[x]/(x^n-1)$ for $n\geq 2$. Then as in Example 5.6 the discriminant algebra $\Delta_{A/\mathbb{Z}}$ has basis $\{1,\dot\gamma^{\mathrm{A}_n}(1,x,\dots,x^{n-1})\}$, and we can present the algebra structure of $\Delta_{A/\mathbb{Z}}$ if we know the trace and norm of $\dot\gamma^{\mathrm{A}_n}(1,x,\dots,x^{n-1})$. The trace is equal to $\Phi_{A/\mathbb{Z}}\big(\gamma^{\mathrm{S}_n}(1,x,\dots,x^{n-1})\big)$, which as in Example 3.3 we can compute as the coefficient of $\lambda_1 \dots \lambda_n$ in the norm of $\lambda_1 + \lambda_2 x + \cdots + \lambda_n x^{n-1}$, which equals the determinant

$$\begin{vmatrix} \lambda_1 & \lambda_n & \lambda_{n-1} & \dots & \lambda_2 \\ \lambda_2 & \lambda_1 & \lambda_n & \ddots & \vdots \\ \lambda_3 & \lambda_2 & \ddots & \ddots & \lambda_{n-1} \\ \vdots & \ddots & \ddots & \lambda_1 & \lambda_n \\ \lambda_n & \dots & \lambda_3 & \lambda_2 & \lambda_1 \end{vmatrix}.$$

This coefficient is equal to the permanent of Schur's matrix $(\zeta^{ij})_{i,j=1}^n$ for ζ a primitive nth root of unity; see [7] for this and the following facts.
For small values of n, the trace of $\dot\gamma^{\mathrm{A}_n}(1, x, \dots, x^{n-1})$ is shown in the following table:

n	2	3	4	5	6	7	8	9	10	11...
Tr	0	−3	0	−5	0	105	0	81	0	6765...

For even n, the trace is always zero; thus $\dot\gamma^{\mathrm{A}_n}(1, x, \dots, x^{n-1})^2$ is in $\mathbb{Z}$ and equals one fourth of the discriminant, so

$$\Delta_{A/\mathbb{Z}} \cong \mathbb{Z}[x]/(x^2 - \frac{1}{4}(-1)^{n/2} n^n),$$

the "naive" discriminant algebra if one remembers the factor of 1/4. But if n is odd, then the trace of $\dot\gamma^{\mathrm{A}_n}(1, x, \dots, x^{n-1})$ is nonzero.

6. Proofs of Theorems 2 to 4

In this section we demonstrate proofs of the other three main theorems from the introduction. First, we show that Theorem 2 holds, so that the operation $(R, A) \mapsto \Delta_{A/R}$ commutes with base change.

THEOREM 6.1. *Let R be a ring, and let A be an R-algebra of rank n with $n \geq 2$. Let R' be an R-algebra, and let $A' = R' \otimes A$, so that A' is an R'-algebra of rank n. The natural R'-algebra isomorphism $R' \otimes (A^{\otimes n})^{\mathrm{A}_n} \to (A'^{\otimes_{R'} n})^{\mathrm{A}_n}$ descends to an R'-algebra isomorphism $R' \otimes \Delta_{A/R} \to \Delta_{A'/R'}$.*

Proof. We proved that the canonical homomorphism $R' \otimes (A^{\otimes n})^{\mathrm{A}_n} \to (A'^{\otimes_{R'} n})^{\mathrm{A}_n}$ is an isomorphism in Proposition 3.5. Then since the Ferrand homomorphism also commutes with base change, we obtain an isomorphism $R' \otimes \Delta_{A/R} \cong \Delta_{A'/R'}$ as desired. □

Second, we can immediately show that satisfying Theorem 3, i.e. the discriminant algebra having the right description when 2 is a unit in the base ring, is a consequence of satisfying Theorem 1, as a corollary of the following proposition:

PROPOSITION 6.2. *Let R be a ring in which 2 is invertible. Let D be an R-algebra of rank 2. Give the rank-2 R-module $R \oplus \bigwedge^2 D$ an R-algebra stucture by making $(1, 0)$ the multiplicative identity and setting $(0, \xi) \cdot (0, \psi) = \frac{1}{4}\delta_D(\xi, \psi)$.*

Then there is a unique isomorphism of R-algebras $D \xrightarrow{\sim} R \oplus \bigwedge^2 D$ inducing the identity map on top exterior powers

$$\bigwedge^2 D \xrightarrow{\sim} \bigwedge^2(R \oplus \bigwedge^2 D) \cong (R \oplus \bigwedge^2 D)/R = \bigwedge^2 D;$$

the isomorphism is $d \mapsto (\frac{1}{2}\mathrm{Tr}_D(d), 1 \wedge d)$.

Proof. First we establish existence. Note that the isomorphism $D/R \xrightarrow{\sim} \bigwedge^2 D$ sending the class of d to $1 \wedge d$ gives us an exact sequence

$$0 \to R \to D \to \bigwedge^2 D \to 0,$$

which is split by the homomorphism $D \to R\colon d \mapsto \frac{1}{2}\mathrm{Tr}_D(d)$. This gives us the desired isomorphism of R-modules $D \cong R \oplus \bigwedge^2 D$ sending d to $(\frac{1}{2}\mathrm{Tr}_D(d), 1 \wedge d)$. Next we show that transporting the R-algebra structure from D to $R \oplus \bigwedge^2 D$ gives the desired multiplication on $R \oplus \bigwedge^2 D$. The image of the multiplicative identity 1 is $(\frac{1}{2}\mathrm{Tr}_D(1), 1 \wedge 1) = (1, 0)$, as desired. All that remains, then, is to check the multiplication on elements of the form $(0, \xi)$, that is, the images of trace-zero elements of D. Then let $d, e \in D$ have trace zero; we will show that $de = \frac{1}{4}\delta_D(1 \wedge d, 1 \wedge e)$ in D. First, note that the squares of d, e, and $d + e$ are all in R: they are roots of their characteristic polynomials, which have no linear term. Therefore $de = \frac{1}{2}((d+e)^2 - d^2 - e^2)$ is in R as well. Then we may compute $\delta_D(1 \wedge d, 1 \wedge e)$ as

$$\delta_D(1 \wedge d, 1 \wedge e) = \det \begin{pmatrix} \mathrm{Tr}_D(1) & \mathrm{Tr}_D(d) \\ \mathrm{Tr}_D(e) & \mathrm{Tr}_D(de) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2de \end{pmatrix} = 4de,$$

so we have $de = \frac{1}{4}\delta_D(1 \wedge d, 1 \wedge e)$ as we wanted to show. Thus the induced product on $R \oplus \bigwedge^2 D$ has $(0, \xi) \cdot (0, \psi) = \frac{1}{4}\delta_D(\xi, \psi)$, as claimed, and we have demonstrated existence of the desired algebra isomorphism.

Now we show that there is only one isomorphism with these properties. It is sufficient to show that the only algebra automorphism of D inducing the identity on $\bigwedge^2 D$ is itself the identity. For this we work locally, so assume D has a basis of the form $\{1, x\}$. An automorphism of D sends x to an element $ux + r$ for some $r \in R$ and u a unit of R. If this is to descend to the identity on $\bigwedge^2 D$, we must have $u = 1$. And if this is an automorphism of D, we must have $\mathrm{Tr}_D(x) = \mathrm{Tr}_D(ux + r) = \mathrm{Tr}_D(x + r) = \mathrm{Tr}_D(x) + 2r$, so $2r = 0$. Since 2 is a unit of R, we have $r = 0$ and the automorphism is id_D. □

Corollary 6.3. *Let R be a ring in which 2 is a unit, and let A be a rank-n R-algebra. Put an R-algebra structure on $R \oplus \bigwedge^n A$ by making $(1, 0)$ the multiplicative identity, and setting $(0, \xi) \cdot (0, \psi) = \frac{1}{4}\delta_A(\xi, \psi)$. Then there is a unique R-algebra isomorphism $\Delta_A \cong R \oplus \bigwedge^n A$ such that the resulting isomorphism $\bigwedge^2 \Delta_A \cong \bigwedge^2(R \oplus \bigwedge^n A) \cong \bigwedge^n A$ is the one from Theorem 4.1.*

Note the extra factor of $\frac{1}{4}$ in the definition of the multiplication, as compared with the statement of Theorem 3 on page 1053. Since 2 is a unit, the two multiplications yield isomorphic algebra structures on $R \oplus \bigwedge^n A$, but we see that the one given here is the one which arises naturally from the identification of the discriminant forms. This is analogous to the factor of $\frac{1}{4}$ one could introduce to the naive discriminant algebra $K[x]/(x^2 - \frac{1}{4}D)$, to make its discriminant D instead of $4D$.

For the remainder of this section, we will suppose that R is *connected*, i.e. that it has exactly two idempotents 0 and 1, so that we are working in the setting of Theorem 4. A finite étale algebra over a connected ring R is automatically an R-algebra of rank n for some natural number n, and a R-algebra A of rank n is finite étale if and only if its discriminant form $\delta_A \colon \bigwedge^n A \times \bigwedge^n A \to R$ is nondegenerate, in the sense that the induced R-module homomorphism

$$\bigwedge^n A \to \mathrm{Hom}(\bigwedge^n A, R)$$

is an isomorphism. It is clear from Theorem 1, then, that A is étale if and only if $\Delta_{A/R}$ is étale, since their discriminant forms are isomorphic.

The significance of finite étale R-algebras is clarified by the following theorem, due to Grothendieck and proven in [8, Ch. V, §7]:

Theorem 6.4. *Let R be a connected ring equipped with a ring homomorphism to a separably closed field K. Then there is a profinite group π_R, called the* fundamental group of R (at K)*, such that for each finite étale R-algebra A, the finite set $F(A) = \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(A, K)$ is naturally equipped with a continuous π_R-action. Furthermore, the assignment $A \mapsto F(A)$ defines a contravariant equivalence of categories*

$$F \colon R\text{-}\mathbf{\acute{e}t} \to \pi_R\text{-}\mathbf{set}$$

from the category of finite étale R-algebras to the category of π_R-sets, i.e. finite sets equipped with a continuous π_R-action.

Note: Grothendieck's original formulation was for the fundamental group of locally Noetherian schemes, but the Noetherian hypothesis is not necessary; an excellent reference is [11, Section 5]. Note also that the fundamental group π_R implicitly depends on the choice of K; different choices of K yield fundamental groups that are isomorphic but not canonically so, a behavior which is analogous to the dependence of the topological fundamental group on a choice of base point. In the following, we will suppress the dependence of π_R on K whenever possible without causing confusion.

Example 6.5. If $R = K$ is a field and K^s is its separable closure, then π_K is naturally identified with the absolute Galois group of K, which acts continuously on $\mathrm{Hom}_{K\text{-}\mathbf{Alg}}(A, K^s)$ for each finite separable K-algebra A.

Remark 6.6. In general, Theorem 6.4 tells us quite a lot about the finite π_R-set corresponding to a given finite étale R-algebra:

(1) For each finite étale R-algebra A, the rank of A is the cardinality of $F(A)$. Indeed, suppose that A is locally free of rank n as an R-module. Then as sets, $F(A) = \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(A, K) \cong \mathrm{Hom}_{K\text{-}\mathbf{Alg}}(K \otimes_R A, K)$, but since $K \otimes_R A$ is a finite separable K-algebra of rank n, it is isomorphic to K^n and there are exactly n K-algebra homomorphisms $K^n \to K$. (In fact, the choice of isomorphism $K \otimes_R A \cong K^n$ amounts to a choice

of bijection $\{1,\dots,n\} \xrightarrow{\sim} F(A)$, so $K \otimes_R A$ is canonically isomorphic to $K^{F(A)}$ as a K-algebra.)

(2) If $A_1,\dots,A_n$ are finite étale R-algebras, then $F(\prod_{i=1}^n A_i)$ is isomorphic to the disjoint union $\coprod_{i=1}^n F(A_i)$, and $F(\bigotimes_{i=1}^n A_i)$ to the product $\prod_{i=1}^n F(A_i)$, each with the induced π_R-action. This is just because a contravariant equivalence sends limits to colimits and vice versa, and products and tensor products of étale algebras are étale.

(3) In particular, the zero R-algebra corresponds to the empty π_R-set, and R itself to a singleton $\{*\}$ with the trivial π_R-action. Then for any finite set S, the *trivial* étale R-algebra $R^S = \prod_{s\in S} R$ corresponds to a π_R-set isomorphic to the set S equipped with the trivial π_R-action.

(4) If G is a finite group acting via R-algebra isomorphisms on a finite étale R-algebra A, then G also acts naturally on the corresponding π_R-set $F(A)$. Furthermore, the R-algebra of G-invariants A^G is also finite étale, and the corresponding π_R-set $F(A^G)$ is isomorphic to $F(A)/G$, the set of G-orbits of $F(A)$. (See [11, Prop. 5.20].)

With these remarks, we will see that the Ferrand homomorphism has an especially nice interpretation in the case of étale algebras:

Proposition 6.7. *Let R be a connected ring equipped with a ring homomorphism to a separably closed field K. Let π_R be the fundamental group. Let A be a finite étale R-algebra corresponding to an n-element π_R-set X under the equivalence of Theorem 6.4. Then the Ferrand homomorphism $\Phi_A\colon (A^{\otimes n})^{\mathrm{S}_n} \to R$ corresponds to the map of π_R-sets $\{*\} \to X^n/\mathrm{S}_n$ sending $*$ to the S_n-orbit of bijections $\{1,\dots,n\} \xrightarrow{\sim} X$.*

Proof. By changing base (to K if necessary) we may assume that A is the trivial étale algebra R^X. Then Ferrand shows in [6, Ex. 3.1.3(b)] that the Ferrand homomorphism $((R^X)^{\otimes n})^{\mathrm{S}_n} \cong R^{X^n/\mathrm{S}_n} \to R$ is projection onto the coordinate indexed by the S_n-orbit of bijections $\{1,\dots,n\} \xrightarrow{\sim} X$. □

Finally, we prove the main theorem of the section.

Theorem 6.8. *Let R be a connected ring with fundamental group π_R, and let A be a finite étale R-algebra corresponding to an n-element π_R-set X, with $n \geq 2$. Then the discriminant algebra Δ_A is a finite étale R-algebra corresponding to the 2-element π_R-set*

$$\mathrm{Or}(X) := \mathrm{Bij}(\{1,\dots,n\}, X)/\mathrm{A}_n$$

of orientations *on X.*

Proof. Note that Δ_A is defined so that the following square is a tensor product diagram:

$$\begin{tikzcd}
\Delta_A & R \arrow[l] \\
(A^{\otimes n})^{\mathrm{A}_n} \arrow[u] & (A^{\otimes n})^{\mathrm{S}_n} \arrow[l] \arrow[u]
\end{tikzcd}$$

Since A is étale, this square is in fact a cofibered product in the category of finite étale R-algebras. Hence under the contravariant equivalence $F\colon R\text{-}\mathbf{\acute{e}t} \to \pi_R\text{-}\mathbf{set}$, this diagram becomes a fiber product diagram of π_R-sets:

$$\begin{array}{ccc} F(\Delta_A) & \longrightarrow & \{*\} \\ \downarrow & & \downarrow \\ X^n/\mathrm{A}_n & \longrightarrow & X^n/\mathrm{S}_n \end{array}$$

This pullback can be computed in the category of sets, and then equipped canonically with a π_R-action. By Proposition 6.7 the image of $*$ in X^n/S_n is the class of bijections $\mathrm{Bij}(\{1,\dots,n\},X)$. So the elements of $F(\Delta_A)$ are A_n-equivalence classes of maps $\{1,\dots,n\} \to X$, whose underlying S_n-equivalence class is $\mathrm{Bij}(\{1,\dots,n\},X)$. In other words, this is the set of A_n-equivalence classes of bijections $\{1,\dots,n\} \xrightarrow{\sim} X$, namely the two-element set $\mathrm{Or}(X)$. $\square$

7. Functoriality

Given an isomorphism of rank-n R-algebras $f\colon A \to B$, we obtain isomorphisms $(f^{\otimes n})^{\mathrm{A}_n}\colon (A^{\otimes n})^{\mathrm{A}_n} \to (B^{\otimes n})^{\mathrm{A}_n}$ and $(f^{\otimes n})^{\mathrm{S}_n}\colon (A^{\otimes n})^{\mathrm{S}_n} \to (B^{\otimes n})^{\mathrm{S}_n}$, and thus an isomorphism of tensor products $\Delta_f\colon \Delta_{A/R} \to \Delta_{B/R}$. The key here is that the following triangle of R-algebra homomorphisms commutes if f is an isomorphism:

$$\begin{tikzcd} (A^{\otimes n})^{\mathrm{S}_n} \arrow[rr, "(f^{\otimes n})^{\mathrm{S}_n}"] \arrow[dr, "\Phi_{A/R}"'] & & (B^{\otimes n})^{\mathrm{S}_n} \arrow[dl, "\Phi_{B/R}"] \\ & R & \end{tikzcd} \tag{3}$$

For a general homomorphism $f\colon A \to B$, if the triangle (3) commutes, then we obtain a homomorphism of discriminant algebras $\Delta_f\colon \Delta_A \to \Delta_B$.

Proposition 7.1. *Let R be a ring, and A and B two R-algebras of rank n. Let $f\colon A \to B$ be an R-algebra homomorphism, and let $\Omega \subseteq A$ be a set of elements of A whose powers generate A as an R-module. Then the following are equivalent:*

(i) The triangle (3) *of R-algebra homomorphisms commutes.*
(ii) For all $a \in A$, we have $\mathrm{Nm}_{A/R}(a) = \mathrm{Nm}_{B/R}(f(a))$, and the same holds after base change to any R-algebra R'.
(iii) For all $a \in \Omega$, the characteristic polynomial of a equals the characteristic polynomial of $f(a)$.

Proof. (i $\Rightarrow$ ii) After base changing to R', we obtain a commuting triangle

$$\begin{tikzcd}
(A'^{\otimes_{R'} n})^{\mathrm{S}_n} \arrow[rr, "(f'^{\otimes n})^{\mathrm{S}_n}"] \arrow[dr, "\Phi_{A'/R'}"'] & & (B'^{\otimes_{R'} n})^{\mathrm{S}_n} \arrow[dl, "\Phi_{B'/R'}"] \\
& R' &
\end{tikzcd}$$

One path sends $a \otimes \cdots \otimes a$ to $\mathrm{Nm}_{A'/R'}(a)$, and other sends it to $\mathrm{Nm}_{B'/R'}(f'(a))$, so these must be equal.
(ii $\Rightarrow$ iii) Given any $a \in A$, we have from (ii) applied to $R' = R[\lambda]$ the equation $\mathrm{Nm}_{A[\lambda]/R[\lambda]}(\lambda - a) = \mathrm{Nm}_{B[\lambda]/R[\lambda]}(\lambda - f(a))$, but these are exactly the characteristic polynomials of a and $f(a)$.
(iii $\Rightarrow$ i) The composite $\Phi_{B/R} \circ (f^{\otimes n})^{\mathrm{S}_n}$ sends $e_k(a) \mapsto e_k(f(a)) \mapsto s_k(f(a)) = s_k(a)$ for each $a \in \Omega$, and therefore equals $\Phi_{A/R}$ by Lemma 3.6. $\square$

We call an R-algebra homomorphism *universally norm-preserving* if it satisfies the equivalent conditions of Proposition 7.1. Isomorphisms are always universally norm-preserving, but the following example shows that universally norm-preserving homomorphisms are in general neither injective nor surjective.

Example 7.2. Let A be any rank-n R-algebra and $a \in A$ any element, with characteristic polynomial $p_a(\lambda) = \mathrm{Nm}_{A[\lambda]/R[\lambda]}(\lambda - a)$. Then the R-algebra homomorphism $R[x]/(p_a(x)) \to A$ sending x to a is universally norm-preserving, since $\Omega = \{x\} \subseteq R[x]/(p_a(x))$ is a set whose powers $\{1, x, x^2, \dots\}$ generate $R[x]/(p_a(x))$ as an R-module, and the characteristic polynomial of x in $R[x]/(p_a(x))$ is again $p_a(\lambda)$.
For example, let r and s be two elements of any ring R. Then we have a universally norm-preserving homomorphism $R[x]/(x-r)(x-s) \to R^2$ sending $x \mapsto (r, s)$. This map is injective if and only if $r - s$ is not a zerodivisor in R, and surjective if and only if $r - s$ is a unit.
Note that there are also well-defined homomorphisms $R[x]/(x-r)(x-s) \to R^2$ sending x to (r, r) or (s, s), but these are not universally norm-preserving unless $r = s$.

Remark 7.3. The S_n-closure operation defined by Bhargava and Satriano in [1] has a universal property related to universally norm-preserving homomorphisms. Namely, a *full set of sections* for a rank-n algebra A is a family of n algebra homomorphisms $A \to R$ such that the resulting homomorphism of rank-n algebras $A \to R^n$ is universally norm-preserving, and the S_n-closure of A over R is the universal R-algebra over which A is equipped with a full set of sections.

8. The discriminant algebra of a product

If A and B are R-algebras of ranks m and n, respectively, then their product $A \times B$ is an R-algebra of rank $m + n$. It is well-known that $\bigwedge^{m+n}(A \times B)$ is canonically isomorphic to $\bigwedge^m A \otimes \bigwedge^n B$, and that if we identify these two locally-free R-modules we find that the discriminant quadratic form $\delta_{A\times B}$ is just $\delta_A \otimes \delta_B$. In this sense, the construction of the discriminant form is multiplicative. We extend this multiplicativity to the construction of the discriminant algebra $\Delta_{A\times B}$.

Namely, for each ring R there is a commutative monoid structure $*_R$ on Quad_R, the set of isomorphism classes of quadratic R-algebras; these monoid structures have recently been characterized by Voight in [19] as the unique family of functions $*_R\colon \mathrm{Quad}_R \times \mathrm{Quad}_R \to \mathrm{Quad}_R$ such that

- For each R, the set Quad_R is a commutative monoid with multiplication $*_R$ and unit the class of R^2,
- For each R-algebra R', the base-change operation $\mathrm{Quad}_R \to \mathrm{Quad}_{R'}$ is a homomorphism of commutative monoids, and
- If S and T are quadratic étale R-algebras with standard involutions σ and τ, then $S *_R T$ is the class of the subring of $S \otimes T$ fixed by $\sigma \otimes \tau$.

In [5], Deligne asserted the existence of such a binary operation over which the discriminant algebra should distribute; an explicit construction of this binary operation on quadratic algebras is due to Loos and can be found in [12].

Our goal in this section is to show that Δ is multiplicative in the sense that $\Delta_{A\times B} \cong \Delta_A * \Delta_B$. Our approach will be to show first that the operation on quadratic algebras $(S,T) \mapsto \Delta_{S\times T}$ satisfies the three properties of the operations $*_R$ listed above, and then to exhibit an isomorphism $\Delta_{A\times B} \cong \Delta_{\Delta_A \times \Delta_B}$. Then we will have

$$\Delta_{A\times B} \cong \Delta_{\Delta_A\times\Delta_B} \cong \Delta_A * \Delta_B.$$

Remark 8.1. The easiest properties to check are base-change and commutativity, and the description in the étale case is also straightforward to verify. Indeed, if S and T are quadratic R-algebras, then $S \times T \cong T \times S$ so by functoriality under isomorphisms we find that

$$\Delta_{S\times T} \cong \Delta_{T\times S}.$$

Furthermore, if R' is any R-algebra, then

$$R' \otimes_R \Delta_{(S\times T)/R} \cong \Delta_{R'\otimes(S\times T)/R'} \cong \Delta_{(S'\times T')/R'},$$

so the operation sending (S,T) to the isomorphism class of $\Delta_{S\times T}$ commutes with base change.

For the étale case, it is sufficient to check in case the base ring R is connected. (Indeed, in the proof of uniqueness in [19] the étale description is only used in a single universal case for which the base ring is even a domain.) Then if we suppose S and T to correspond to π_R-sets X and Y, to check that $(S\otimes T)^{\mathrm{S}_2}$ is isomorphic to $\Delta_{S\times T}$ we need only find an isomorphism of π_R-sets

$$(X\times Y)/\mathrm{S}_2 \cong \mathrm{Bij}\big(\{1,\dots,4\}, X\sqcup Y\big)/\mathrm{A}_4.$$

To wit, we have isomorphisms $X \cong \mathrm{Bij}(\{1,2\},X)$ and $Y \cong \mathrm{Bij}(\{3,4\},Y)$, and an inclusion

$$\mathrm{Bij}(\{1,2\},X)\times\mathrm{Bij}(\{3,4\},Y) \hookrightarrow \mathrm{Bij}\big(\{1,\dots,4\},X\sqcup Y\big).$$

It is easy to check that after projecting to $\mathrm{Bij}\big(\{1,\dots,4\}, X\sqcup Y\big)/\mathrm{A}_4$, we obtain a well-defined bijection from $\big(\mathrm{Bij}(\{1,2\},X)\times\mathrm{Bij}(\{3,4\},Y)\big)/\mathrm{S}_2$.

Checking that the operation $(S,T)\mapsto \Delta_{S\times T}$ is associative and has unit R^2, and that there is an isomorphism $\Delta_{A\times B}\cong\Delta_{\Delta_A\times\Delta_B}$ for general A and B, will occupy the rest of this section. To check these statements, we will have to dig into explicit computations with elements.
We use the following abuse of notation in the hope that it will prevent the reader from being buried by parentheses. In product algebras of the form $A\times B$, we will often need to refer to elements of the form $(a,0)$ or $(0,b)$. We will usually denote such elements simply by a or b, thus implicitly identifying the rings A and B with their corresponding ideals $A\times 0$ and $0\times B$ in $A\times B$. Since each of A and B naturally contains an image of R, for each $r\in R$ we will write r_A for $(r,0)$ and r_B for $(0,r)$; thus the two idempotents $(1,0)$ and $(0,1)$ in $A\times B$ are 1_A and 1_B, respectively, and their sum is the unit 1.

Remark 8.2. For example, in this notation the isomorphism

$$\textstyle\bigwedge^m A\otimes\bigwedge^n B\cong\bigwedge^{(m+n)}(A\times B)$$

is the one sending $(a_1\wedge\cdots\wedge a_m)\otimes(b_1\wedge\cdots\wedge b_n)\mapsto a_1\wedge\cdots\wedge a_m\wedge b_1\wedge\cdots\wedge b_n$ for all $a_1,\dots,a_m\in A$ and $b_1,\dots,b_n\in B$ (see [2, Prop. 10 on p. III.84]).

Remark 8.3. As a consequence, $\Delta_{A\times B}$ is generated as an R-module by 1 together with elements of the form $\dot\gamma^{\mathrm{A}_{m+n}}(a_1,\dots,a_m,b_1,\dots,b_n)$ with $a_1,\dots,a_m\in A$ and $b_1,\dots,b_n\in B$ by Remark 5.3. We will usually write such an element as $\dot\gamma^{\mathrm{A}_{m+n}}(a,b)$, where $a=(a_1,\dots,a_m)\in A^m$ and $b=(b_1,\dots,b_n)\in B^n$.

We will also often use the following description of the Ferrand homomorphism for $A\times B$:

Lemma 8.4. *Let R be a ring, and let A and B be R-algebras of ranks m and n, respectively. Identify S_m and S_n with subgroups of S_{m+n} permuting the first m and last n elements of $\{1,\dots,m+n\}$, respectively.*

(1) For each subgroup $G\subseteq\mathrm{S}_{m+n}$, the R-algebra projection

$$\pi\colon (A\times B)^{\otimes m+n}\to A^{\otimes m}\otimes B^{\otimes n}$$

sending $(a_1,b_1)\otimes\cdots\otimes(a_{m+n},b_{m+n})$ to $(a_1\otimes\cdots\otimes a_m)\otimes(b_{m+1}\otimes\cdots\otimes b_{m+n})$ restricts to an R-algebra homomorphism

$$((A\times B)^{\otimes(m+n)})^G\to(A^{\otimes m})^{G\cap\mathrm{S}_m}\otimes(B^{\otimes n})^{G\cap\mathrm{S}_n}.$$

(2) In case $G=\mathrm{S}_{m+n}$, the resulting composite

$$((A\times B)^{\otimes(m+n)})^{\mathrm{S}_{m+n}}\to(A^{\otimes m})^{\mathrm{S}_m}\otimes(B^{\otimes n})^{\mathrm{S}_n}\xrightarrow{\Phi_A\otimes\Phi_B}R\otimes R\cong R$$

is the Ferrand homomorphism $\Phi_{A\times B}$.

Proof. (1) Set $H = G \cap \mathrm{S}_m$ and $K = G \cap \mathrm{S}_n$. Then $H \times K$ is naturally a subgroup of G, and we have an inclusion

$$((A \times B)^{\otimes(m+n)})^G \hookrightarrow ((A \times B)^{\otimes(m+n)})^{H\times K}.$$

Thus it is enough to show that $\pi\colon (A \times B)^{\otimes(m+n)} \to A^{\otimes m} \otimes B^{\otimes n}$ restricts to a homomorphism $((A \times B)^{\otimes(m+n)})^{H\times K} \to (A^{\otimes m})^H \otimes (B^{\otimes n})^K$. Now $\mathrm{S}_m \times \mathrm{S}_n$ acts on both $(A \times B)^{\otimes m+n}$ and $A^{\otimes m} \otimes B^{\otimes n}$ by permuting the first m and last n tensor factors separately, and the projection π is equivariant with respect to this action. Thus we obtain a map of $H \times K$-invariants

$$((A \times B)^{\otimes(m+n)})^{H\times K} \to \left(A^{\otimes m} \otimes B^{\otimes n}\right)^{H\times K}.$$

Finally, observe that $\left(A^{\otimes m} \otimes B^{\otimes n}\right)^{H\times K} = (A^{\otimes m})^H \otimes (B^{\otimes n})^K$ as subalgebras of $A^{\otimes m} \otimes B^{\otimes n}$. (By Proposition 3.5, this can be checked after changing base to a localization in which both A and B are free R-modules, in which case the isomorphism is elementary.) Thus we have obtained the desired homomorphism as the composite

$$((A \times B)^{\otimes(m+n)})^G \hookrightarrow ((A \times B)^{\otimes(m+n)})^{H\times K} \to (A^{\otimes m})^H \otimes (B^{\otimes n})^K.$$

(2) We check the defining property of $\Phi_{A\times B}$. Let (a, b) be an arbitrary element of $A\times B$; is $(a, b)\otimes\cdots\otimes(a, b)$ sent to $\mathrm{Nm}_{A\times B}(a, b) = \mathrm{Nm}_A(a)\mathrm{Nm}_B(b)$? Indeed so: we have

$$\begin{aligned}(a, b) \otimes \cdots \otimes (a, b) &\mapsto (a \otimes \cdots \otimes a) \otimes (b \otimes \cdots \otimes b)\\ &\mapsto (\mathrm{Nm}_A(a)) \otimes (\mathrm{Nm}_B(b))\\ &\mapsto \mathrm{Nm}_A(a)\mathrm{Nm}_B(b)\end{aligned}$$

as desired. The same property holds also after base change, so the indicated homomorphism is $\Phi_{A\times B}$. □

Our first application is to check that R^2 is a unit for the operation $(S, T) \mapsto \Delta_{S\times T}$. More generally, if A is any rank-n R-algebra, then we have the following R-algebra isomorphism $\Delta_{R\times A} \cong \Delta_A$:

Theorem 8.5. *Let R be a ring, and let A be an R-algebra of rank $n \geq 2$. The R-algebra homomorphism $(R \times A)^{\otimes(n+1)} \to A^{\otimes n}$ sending*

$$(r_0, a_0) \otimes (r_1, a_1) \otimes \cdots \otimes (r_n, a_n) \mapsto r_0 \cdot (a_1 \otimes \cdots \otimes a_n)$$

restricts to an R-algebra homomorphism $((R \times A)^{\otimes(n+1)})^{\mathrm{A}_{n+1}} \to (A^{\otimes n})^{\mathrm{A}_n}$ that descends to an R-algebra isomorphism $\Delta_{R\times A} \to \Delta_A$.

Proof. The homomorphism $(R \times A)^{\otimes n+1} \to A^{\otimes n} \cong R^{\otimes 1} \otimes A^{\otimes n}$ is of the form considered in Lemma 8.4(1), with R and A in place of A and B. Using the subgroup $\mathrm{A}_{n+1} \subseteq \mathrm{S}_{n+1}$, whose intersection with S_n is A_n, Lemma 8.4(1) tells us that the homomorphism restricts to one

$$((R \times A)^{\otimes(n+1)})^{\mathrm{A}_{n+1}} \to R \otimes (A^{\otimes n})^{\mathrm{A}_n} \cong (A^{\otimes n})^{\mathrm{A}_n},$$

as desired. In addition, we know from Lemma 8.4(2) that the further restriction $((R \times A)^{\otimes(n+1)})^{\mathrm{S}_{n+1}} \to (A^{\otimes n})^{\mathrm{S}_n}$ commutes with the Ferrand homomorphisms to R; thus we obtain a morphism of tensor products

$$((R\times A)^{\otimes(n+1)})^{\mathrm{A}_{n+1}} \bigotimes_{((R\times A)^{\otimes(n+1)})^{\mathrm{S}_{n+1}}} R \to (A^{\otimes n})^{\mathrm{A}_n} \bigotimes_{(A^{\otimes n})^{\mathrm{S}_n}} R,$$

i.e. an R-algebra homomorphism $\Delta_{R\times A} \to \Delta_A$.
To show that this homomorphism is an isomorphism, we show that it fits into a map of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & R \arrow[r] \arrow[d, equal] & \Delta_{R\times A} \arrow[r] \arrow[d] & \bigwedge^{n+1}(R\times A) \arrow[r] & 0 \\
0 \arrow[r] & R \arrow[r] & \Delta_A \arrow[r] & \bigwedge^n A \arrow[r] \arrow[u, "\sim"] & 0
\end{tikzcd}$$

where the right-hand isomorphism is the one $\bigwedge^n A \cong \bigwedge^1 R \otimes \bigwedge^n A \cong \bigwedge^{n+1}(R \times A)$ from Remark 8.2. The left-hand square commutes because $\Delta_{R\times A} \to \Delta_A$ is an R-algebra homomorphism. To show that the right-hand square commutes, follow an element $\dot\gamma^{\mathrm{A}_{n+1}}(1_R, a_1, \ldots, a_n)$ of $\Delta_{R\times A}$; such elements along with 1 generate $\Delta_{R\times A}$ by Remark 8.3. Its image in Δ_A is $\dot\gamma^{\mathrm{A}_n}(a_1, \ldots, a_n)$, giving $a_1 \wedge \cdots \wedge a_n$ in $\bigwedge^n A$, thence $1_R \wedge a_1 \wedge \cdots \wedge a_n$ in $\bigwedge^{n+1}(R \times A)$. But this corresponds exactly to the action of the homomorphism $\Delta_{R\times A} \to \bigwedge^{n+1}(R\times A)$. Thus the right-hand square commutes as well, so by the Five Lemma, the homomorphism $\Delta_{R\times A} \to \Delta_A$ is an isomorphism of R-algebras. □

Remark 8.6. Certain authors (such as Deligne in [5] and Loos in [13]) construct a discriminant algebra for only even-rank or only odd-rank algebras, defining the discriminant algebra of an algebra A whose rank is of the wrong parity to be that of $R\times A$. The fact that our construction is invariant under adding a factor of R will be useful in future work comparing these different constructions.

Remark 8.7. Note that we thus have an isomorphism $\Delta_A \cong \Delta_{R^2\times A}$ for all R-algebras of rank at least 2, but the right-hand side is also well-defined for R-algebras of rank 0 or 1, and is then isomorphic to R^2. In this way we can extend the domain of the discriminant algebra operation to all constant rank (and even locally constant rank) algebras.

All that remains, then, to show that $\Delta_{S\times T} \cong S * T$ is to check that the operation $(S, T) \mapsto \Delta_{S\times T}$ is associative. This will follow from our exhibiting an isomorphism $\Delta_{A\times B} \cong \Delta_{\Delta_A\times\Delta_B}$, for then

$$\Delta_{S\times\Delta_{T\times U}} \cong \Delta_{\Delta_S\times\Delta_{T\times U}} \cong \Delta_{S\times(T\times U)} \cong$$
$$\cong \Delta_{(S\times T)\times U} \cong \Delta_{\Delta_{S\times T}\times\Delta_U} \cong \Delta_{\Delta_{S\times T}\times U},$$

where we have used the isomorphisms $S \cong \Delta_S$ and $U \cong \Delta_U$ from Proposition 5.1. So without any more ado, here is the promised isomorphism:

Theorem 8.8. *Let R be a ring, and let A and B be R-algebras of ranks m and n, respectively, with both m and n at least 2. Then there is a unique R-algebra isomorphism $\Delta_{A\times B} \xrightarrow{\sim} \Delta_{\Delta_A\times\Delta_B}$ that sends $1\mapsto 1$ and $\dot\gamma^{\mathrm{A}_{m+n}}(a,b)$ to $\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A}, \dot\gamma^{\mathrm{A}_m}(a), 1_{\Delta_B}, \dot\gamma^{\mathrm{A}_n}(b)\big)$ for each $a\in A^m$ and $b\in B^n$.*

The proof that this assignment describes a well-defined algebra isomorphism is long and unenlightening. The authors hope that future work will reveal a simpler construction of this isomorphism that avoids the elementary slog to follow. Indeed, for the proof we use the following lemma several times:

Lemma 8.9. *Let $a=(a_1,\ldots,a_m)\in A^m$ and $b=(b_1,\ldots,b_n)\in B^n$. Then*

$$\Phi_{A\times B}\big(\gamma^{\mathrm{S}_{m+n}}(a,b)\big) = \Phi_A\big(\gamma^{\mathrm{S}_m}(a)\big)\cdot\Phi_B\big(\gamma^{\mathrm{S}_n}(b)\big).$$

If two of the a_i are equal, then $\gamma^{\mathrm{A}_{m+n}}(a,b)$ is S_{m+n}-invariant, and

$$\Phi_{A\times B}\big(\gamma^{\mathrm{A}_{m+n}}(a,b)\big) = \Phi_A\big(\gamma^{\mathrm{A}_m}(a)\big)\cdot\Phi_B\big(\gamma^{\mathrm{S}_n}(b)\big).$$

Proof. By Lemma 8.4(2), the Ferrand homomorphism for $A\times B$ may be computed by first projecting to $(A^{\otimes m})^{\mathrm{S}_m}\otimes(B^{\otimes n})^{\mathrm{S}_n}$ and then applying $\Phi_A\otimes\Phi_B$. In our case, the terms of $\gamma^{\mathrm{S}_{m+n}}(a,b)$ that survive after the projection are exactly those with the a_i among the first m tensor factors and the b_i among the last n. Thus the image of $\gamma^{\mathrm{S}_{m+n}}(a,b)$ in $(A^{\otimes m})^{\mathrm{S}_m}\otimes(B^{\otimes n})^{\mathrm{S}_n}$ is $\gamma^{\mathrm{S}_m}(a)\otimes\gamma^{\mathrm{S}_n}(b)$. Therefore

$$\Phi_{A\times B}\big(\gamma^{\mathrm{S}_{m+n}}(a,b)\big) = \Phi_A\big(\gamma^{\mathrm{S}_m}(a)\big)\cdot\Phi_B\big(\gamma^{\mathrm{S}_n}(b)\big)$$

as desired.

If two of the a_i are equal, then the image of $\gamma^{\mathrm{A}_{m+n}}(a,b)$ after projecting to $A^{\otimes m}\otimes B^{\otimes n}$ is the sum $\gamma^{\mathrm{A}_m}(a)\otimes\gamma^{\mathrm{A}_n}(b)+\gamma^{\overline{\mathrm{A}}_m}(a)\otimes\gamma^{\overline{\mathrm{A}}_n}(b)$, which equals $\gamma^{\mathrm{A}_m}(a)\otimes\gamma^{\mathrm{S}_n}(b)$ since $\gamma^{\mathrm{A}_m}(a)=\gamma^{\overline{\mathrm{A}}_m}(a)$. Thus we obtain

$$\Phi_{A\times B}\big(\gamma^{\mathrm{A}_{m+n}}(a,b)\big) = \Phi_A\big(\gamma^{\mathrm{A}_m}(a)\big)\cdot\Phi_B\big(\gamma^{\mathrm{S}_n}(b)\big)$$

as claimed. ☐

Example 8.10. As a special case, consider quadratic R-algebras S and T with $s\in S$ and $t\in T$. We have

$$\begin{aligned}\Phi_{S\times T}\big(\gamma^{\mathrm{A}_4}(s,s,1_T,t)\big) &= \Phi_S\big(\gamma^{\mathrm{A}_2}(s,s)\big)\cdot\Phi_T\big(\gamma^{\mathrm{S}_2}(1,t)\big)\\ &= \Phi_S(s\otimes s)\cdot\Phi_T(1\otimes t+t\otimes 1)\\ &= \mathrm{Nm}_S(s)\cdot\mathrm{Tr}_T(t).\end{aligned}\tag{4}$$

Similarly, we have

$$\begin{aligned}\Phi_{S\times T}\big(\gamma^{\mathrm{A}_4}(s,s,t,t)\big) &= \Phi_S\big(\gamma^{\mathrm{A}_2}(s,s)\big)\cdot\Phi_T\big(\gamma^{\mathrm{S}_2}(t,t)\big)\\ &= \Phi_S(s\otimes s)\cdot\Phi_T(t\otimes t+t\otimes t)\\ &= \mathrm{Nm}_S(s)\cdot 2\mathrm{Nm}_T(t)\\ &= 2\mathrm{Nm}_S(s)\mathrm{Nm}_T(t).\end{aligned}\tag{5}$$

These two identities will come up again in the proof of Theorem 8.8.

Proof of Theorem 8.8. For uniqueness, note that $\Delta_{A\times B}$ is generated as an R-module by 1 and elements of the form $\dot\gamma^{\mathrm{A}_{m+n}}(a_1,\dots,a_m,b_1,\dots,b_n)$ by Remark 8.3. We demonstrate the existence of such an isomorphism on each localization of R under which A and B become free R-modules. By uniqueness, then, these isomorphisms on the localizations will glue to an R-algebra isomorphism between the two original discriminant algebras.

Thus it suffices to assume A and B are free, say with R-bases $\theta=(\theta_1,\dots,\theta_m)$ and $\phi=(\phi_1,\dots,\phi_n)$, respectively. In that case, $\Delta_{A\times B}$ is freely generated as an R-module by 1 and $\dot\gamma^{\mathrm{A}_{m+n}}(\theta_1,\dots,\theta_m,\phi_1,\dots,\phi_n)$; we abbreviate the latter as $\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)$. Similarly, $\Delta_{\Delta_A\times\Delta_B}$ is freely generated as an R-module by 1 and $\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big)$. Then we can naively define an R-module isomorphism

$$f\colon \Delta_{A\times B}\to\Delta_{\Delta_A\times\Delta_B}$$

sending $1\mapsto 1$ and $\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)\mapsto\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big)$. We claim that in fact

$$f\colon \dot\gamma^{\mathrm{A}_{m+n}}(a,b)\mapsto\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(a),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b)\big)$$

for all $a=(a_1,\dots,a_m)\in A^m$ and $b=(b_1,\dots,b_n)\in B^n$, so that f acts elementwise as desired. Then we will show that f is multiplicative, making it an R-algebra isomorphism.

Since the expressions $\dot\gamma^{\mathrm{A}_{m+n}}(a,b)$ and $\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(a),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b)\big)$ are each multilinear in the a_i and b_j, we can reduce to proving the claim in case each of the a_i and b_j are among the basis elements for A and B.

The first possibility is that two of the a_i or two of the b_j are equal. Without loss of generality, assume that the a_i are not all distinct. Then $\gamma^{\mathrm{A}_{m+n}}(a,b)$ is S_{m+n}-invariant and $\dot\gamma^{\mathrm{A}_{m+n}}(a,b)$ is equal to $\Phi_{A\times B}\big(\gamma^{\mathrm{A}_{m+n}}(a,b)\big)=\Phi_A\big(\gamma^{\mathrm{A}_m}(a)\big)\Phi_B\big(\gamma^{\mathrm{S}_n}(b)\big)$ by Lemma 8.9.

On the other hand, since $\gamma^{\mathrm{A}_m}(a)\in(A^{\otimes m})^{\mathrm{A}_m}$ is also S_m-invariant, we can also express $\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(a),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b)\big)$ in a form amenable to the Example 8.10 identities:

$$\begin{aligned}\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(a),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b)\big)&=\dot\gamma^{\mathrm{A}_4}\Big(1_{\Delta_A},\Phi_A\big(\gamma^{\mathrm{A}_m}(a)\big)_{\Delta_A},1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b)\Big)\\&=\Phi_A\big(\gamma^{\mathrm{A}_m}(a)\big)\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},1_{\Delta_A},1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b)\big)\\&=\Phi_A\big(\gamma^{\mathrm{A}_m}(a)\big)\mathrm{Nm}_{\Delta_A}(1)\mathrm{Tr}_{\Delta_B}\big(\dot\gamma^{\mathrm{A}_n}(b)\big)\\&=\Phi_A\big(\gamma^{\mathrm{A}_m}(a)\big)\Phi_B\big(\gamma^{\mathrm{S}_n}(b)\big).\end{aligned}$$

Therefore in this case f sends $\dot\gamma^{\mathrm{A}_{m+n}}(a,b)$ to $\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(a),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b)\big)$ because these two elements are the same R-multiple of 1.

The second possibility is that the a_i are a permutation of the θ_i, and the b_j are a permutation of the ϕ_j. Write $a=\theta_\sigma$ and $b=\phi_\tau$ for appropriate permutations $\sigma\in\mathrm{S}_m$ and $\tau\in\mathrm{S}_n$, recalling the notation from Lemma 3.7 for the action of the symmetric group on the set of tuples. We must show that

$$f\colon \dot\gamma^{\mathrm{A}_{m+n}}(\theta_\sigma,\phi_\tau)\mapsto\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta_\sigma),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi_\tau)\big).$$

There are four cases, according to the signs of σ and τ, which determine the values of $\dot\gamma^{\mathrm{A}_{m+n}}(\theta_\sigma,\phi_\tau)$, $\dot\gamma^{\mathrm{A}_m}(\theta_\sigma)$, and $\dot\gamma^{\mathrm{A}_n}(\phi_\tau)$. So we must show that the following four assignments hold:

$$f\colon \dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)\mapsto \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big), \text{ from } \sigma \text{ and } \tau \text{ even,}$$
$$f\colon \dot\gamma^{\overline{\mathrm{A}}_{m+n}}(\theta,\phi)\mapsto \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\overline{\mathrm{A}}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big), \text{ from } \sigma \text{ odd and } \tau \text{ even,}$$
$$f\colon \dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)\mapsto \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\overline{\mathrm{A}}_m}(\theta),1_{\Delta_B},\dot\gamma^{\overline{\mathrm{A}}_n}(\phi)\big), \text{ from } \sigma \text{ and } \tau \text{ odd, and}$$
$$f\colon \dot\gamma^{\overline{\mathrm{A}}_{m+n}}(\theta,\phi)\mapsto \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta),1_{\Delta_B},\dot\gamma^{\overline{\mathrm{A}}_n}(\phi)\big), \text{ from } \sigma \text{ even and } \tau \text{ odd.}$$

The first of the four assignments holds by the definition of f. As for the others, note that

$$\begin{aligned}\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)+\dot\gamma^{\overline{\mathrm{A}}_{m+n}}(\theta,\phi) &= \dot\gamma^{\mathrm{S}_{m+n}}(\theta,\phi)\\ &= \Phi_{A\times B}\left(\gamma^{\mathrm{S}_{m+n}}(\theta,\phi)\right)\\ &= \Phi_A\left(\gamma^{\mathrm{S}_m}(\theta)\right)\Phi_B\left(\gamma^{\mathrm{S}_n}(\phi)\right),\end{aligned}$$

so it is enough to show that the sum of each successive pair of outputs is $\Phi_A\left(\gamma^{\mathrm{S}_m}(\theta)\right)\Phi_B\left(\gamma^{\mathrm{S}_n}(\phi)\right)$. And this indeed holds: for example,

$$\begin{aligned}&\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big)+\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\overline{\mathrm{A}}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big)\\ &\quad= \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta)+\dot\gamma^{\overline{\mathrm{A}}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big)\\ &\quad= \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{S}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big)\\ &\quad= \dot\gamma^{\mathrm{A}_4}\left(1_{\Delta_A},\Phi_A\left(\gamma^{\mathrm{S}_m}(\theta)\right)_{\Delta_A},1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\right)\\ &\quad= \Phi_A\left(\gamma^{\mathrm{S}_m}(\theta)\right)\dot\gamma^{\mathrm{A}_4}\left(1_{\Delta_A},1_{\Delta_A},1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\right)\\ &\quad= \Phi_A\left(\gamma^{\mathrm{S}_m}(\theta)\right)\mathrm{Nm}_{\Delta_A}(1)\,\mathrm{Tr}_{\Delta_B}\left(\dot\gamma^{\mathrm{A}_n}(\phi)\right)\\ &\quad= \Phi_A\left(\gamma^{\mathrm{S}_m}(\theta)\right)\Phi_B\left(\gamma^{\mathrm{S}_n}(\phi)\right).\end{aligned}$$

The other two sums can be evaluated similarly. So indeed, we have shown that f must send $\dot\gamma^{\mathrm{A}_{m+n}}(\theta_\sigma,\phi_\tau)$ to $\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta_\sigma),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi_\tau)\big)$, and established the claim that

$$f\colon \dot\gamma^{\mathrm{A}_{m+n}}(a,b)\mapsto \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(a),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b)\big)$$

for all $a\in A^m$ and $b\in B^n$.

Now we show that the R-module isomorphism $f\colon \Delta_{A\times B}\to\Delta_{\Delta_A\times\Delta_B}$ is in fact an R-algebra isomorphism. Since f is R-linear and $\{1,\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)\}$ forms an R-basis for $\Delta_{A\times B}$, all that we need to check is whether

$$\begin{gathered} f(1\cdot 1)=f(1)\cdot f(1),\\ f(1\cdot\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi))=f(1)\cdot f(\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)), \text{ and}\\ f(\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)\cdot\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi))=f(\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi))\cdot f(\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)).\end{gathered}$$

The first two hold because $f(1)=1$ by definition, so all that is left to check is that $f\left(\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)\right)^2 = f\left(\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)^2\right)$. Now we can use Lemma 3.7 to expand this product:

$$\begin{aligned}\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)^2 &= \sum_{\sigma\in\mathrm{A}_{m+n}} \dot\gamma^{\mathrm{A}_{m+n}}\big((\theta,\phi)(\theta,\phi)_\sigma\big)\\ &= \sum_{\substack{(\sigma,\tau)\in\\ (\mathrm{A}_m\times\mathrm{A}_n)\cup(\overline{\mathrm{A}}_m\times\overline{\mathrm{A}}_n)}} \dot\gamma^{\mathrm{A}_{m+n}}(\theta\theta_\sigma,\phi\phi_\tau),\end{aligned}$$

since $(\theta,\phi)(\theta,\phi)_\sigma$ has a zero entry unless σ belongs to $\mathrm{A}_{m+n}\cap(\mathrm{S}_m\times\mathrm{S}_n) = (\mathrm{A}_m\times\mathrm{A}_n)\cup(\overline{\mathrm{A}}_m\times\overline{\mathrm{A}}_n)$. Therefore

$$\begin{aligned}f\left(\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)^2\right) &= \sum_{\substack{(\sigma,\tau)\in\\ (\mathrm{A}_m\times\mathrm{A}_n)\cup(\overline{\mathrm{A}}_m\times\overline{\mathrm{A}}_n)}} \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta\theta_\sigma),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi\phi_\tau)\big)\\ &= \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta)^2,1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)^2\big)\\ &\quad+\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta)\dot\gamma^{\overline{\mathrm{A}}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\dot\gamma^{\overline{\mathrm{A}}_n}(\phi)\big).\end{aligned}$$

On the other hand,

$$\begin{aligned}f\left(\dot\gamma^{\mathrm{A}_{m+n}}(\theta,\phi)\right)^2 &= \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\big)^2\\ &= \dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta)^2,1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)^2\big)\\ &\quad+\dot\gamma^{\mathrm{A}_4}\big(\dot\gamma^{\mathrm{A}_m}(\theta),\dot\gamma^{\mathrm{A}_m}(\theta),\dot\gamma^{\mathrm{A}_n}(\phi),\dot\gamma^{\mathrm{A}_n}(\phi)\big),\end{aligned}$$

by a similar application of Lemma 3.7. One of each of the two terms on the right-hand sides matches immediately, but the others are also equal:

$$\begin{aligned}&\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(\theta)\dot\gamma^{\overline{\mathrm{A}}_m}(\theta),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(\phi)\dot\gamma^{\overline{\mathrm{A}}_n}(\phi)\big)\\ &= \dot\gamma^{\mathrm{A}_4}\left(1_{\Delta_A},\mathrm{Nm}_{\Delta_A}\big(\dot\gamma^{\mathrm{A}_m}(\theta)\big)_{\Delta_A},1_{\Delta_B},\mathrm{Nm}_{\Delta_B}\big(\dot\gamma^{\mathrm{A}_n}(\phi)\big)_{\Delta_B}\right)\\ &= \mathrm{Nm}_{\Delta_A}\big(\dot\gamma^{\mathrm{A}_m}(\theta)\big)\,\mathrm{Nm}_{\Delta_B}\big(\dot\gamma^{\mathrm{A}_n}(\phi)\big)\,\dot\gamma^{\mathrm{A}_4}\left(1_{\Delta_A},1_{\Delta_A},1_{\Delta_B},1_{\Delta_B}\right)\\ &= 2\,\mathrm{Nm}_{\Delta_A}\big(\dot\gamma^{\mathrm{A}_m}(\theta)\big)\,\mathrm{Nm}_{\Delta_B}\big(\dot\gamma^{\mathrm{A}_n}(\phi)\big)\\ &= \dot\gamma^{\mathrm{A}_4}\big(\dot\gamma^{\mathrm{A}_m}(\theta),\dot\gamma^{\mathrm{A}_m}(\theta),\dot\gamma^{\mathrm{A}_n}(\phi),\dot\gamma^{\mathrm{A}_n}(\phi)\big).\end{aligned}$$

Thus f is an R-algebra isomorphism $\Delta_{A\times B}\to\Delta_{\Delta_A\times\Delta_B}$, as desired. □

Remark 8.11. The isomorphism of Theorem 8.8 does not entirely commute with the isomorphisms interchanging A and B. While it is always the case that

$$\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(a_1,\ldots,a_m),1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b_1,\ldots,b_n)\big)$$

equals

$$\dot\gamma^{\mathrm{A}_4}\big(1_{\Delta_B},\dot\gamma^{\mathrm{A}_n}(b_1,\ldots,b_n),1_{\Delta_A},\dot\gamma^{\mathrm{A}_m}(a_1,\ldots,a_m)\big),$$

the elements $\dot\gamma^{\mathrm{A}_{m+n}}(a_1,\ldots,a_m,b_1,\ldots,b_n)$ and $\dot\gamma^{\mathrm{A}_{m+n}}(b_1,\ldots,b_n,a_1,\ldots,a_m)$ are generally only equal if m or n is even; otherwise they are conjugates. Thus the chain of isomorphisms

$$\Delta_{A\times B}\cong\Delta_{\Delta_A\times\Delta_B}\cong\Delta_{\Delta_B\times\Delta_A}\cong\Delta_{B\times A}\cong\Delta_{A\times B}$$

is the identity if the rank of A or B is even, but is the standard involution on $\Delta_{A\times B}$ if the ranks of A and B are both odd. This is precisely the behavior described by Deligne at the end of [5].

References

[1] Bhargava, M., and Satriano, M. On a notion of "Galois closure" for extensions of rings. *Journal of the European Mathematical Society 16*, 9 (2014), 1881–1913.

[2] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris, 1970.

[3] Bourbaki, N. *Éléments de mathématique. Algèbre commutative. Chapitres 1 à 4*, vol. 1. Springer, 1998.

[4] Deligne, P. *Cohomologie a supports propres.* Springer, 1973.

[5] Deligne, P. Letter to M. Rost and M. Bhargava. Available at `http://pub.math.leidenuniv.nl/~bieselod/references/deligneletter.pdf`, 2005.

[6] Ferrand, D. Un foncteur norme. *Bull. Soc. Math. France 126*, 1 (1998), 1–49.

[7] Graham, R., and Lehmer, D. On the permanent of Schur's matrix. *Journal of the Australian Mathematical Society (Series A) 21*, 04 (1976), 487–497.

[8] Grothendieck, A. *Revêtements étales et groupe fondamental (SGA 1).* Documents Mathématiques (Paris), 3. Société Mathématique de France, Paris, 2003.

[9] Katz, N. M., and Mazur, B. *Arithmetic moduli of elliptic curves*, vol. 108 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 1985.

[10] Knus, M.-A., Merkurjev, A., Rost, M., and Tignol, J.-P. *The Book of Involutions*, vol. 44. Amer. Math. Soc., 1998.

[11] Lenstra, H. W. Galois theory for schemes. Available at `http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`, 2008.

[12] Loos, O. Tensor products and discriminants of unital quadratic forms over commutative rings. *Monatshefte für Mathematik 122*, 1 (1996), 45–98.

[13] Loos, O. Discriminant algebras of finite rank algebras and quadratic trace modules. *Math. Z. 257*, 3 (2007), 467–523.

[14] Roby, N. Lois polynomes et lois formelles en théorie des modules. *Ann. Sci. École Norm. Sup. (3) 80* (1963), 213–348.

[15] Roby, N. Lois polynômes multiplicatives universelles. *C. R. Acad. Sci. Paris Sér. A-B 290*, 19 (1980), A869–A871.

[16] Rost, M. The discriminant algebra of a cubic algebra. Available at `http://www.math.uni-bielefeld.de/~rost/data/cub-disc.pdf`, 2002.

[17] Vaccarino, F. Generalized symmetric functions and invariants of matrices. *Mathematische Zeitschrift 260*, 3 (2008), 509–526.

[18] Voight, J. Rings of low rank with a standard involution. *Illinois Journal of Mathematics 55*, 3 (2011), 1135–1154.

[19] Voight, J. Discriminants and the monoid of quadratic rings. *ArXiv e-prints* (Apr. 2015).

[20] Waterhouse, W. C. Discriminants of etale algebras and related structures. *J. reine angew. Math 379* (1987), 209–220.

Owen Biesel
Mathematisch Instituut
Niels Bohrweg 1
Leiden University
The Netherlands.
bieselod@math.leidenuniv.nl

Alberto Gioia
alberto.gioia@univie.ac.at